NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AUTHENTICATION SCENARIO FOR CYBERCIEGE

by

David S. Mueller

September 2005

Thesis Co-Advisors:	Cynthia E. Irvine
	Paul C. Clark
Second Reader:	Michael F. Thompson

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Authentication Scenario for CyberCIEGE			**5. FUNDING NUMBERS**
6. AUTHOR(S) David S. Mueller			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Frequent media reports of the loss or compromise of data stored on computer systems indicate that attempts to educate users on proper computer security policies and procedures seem to be ineffective. In an effort to provide a means of education that will more fully engage users, the CyberCIEGE game was created. It is hoped that by playing CyberCIEGE users will absorb computer security concepts better than they have through more traditional forms of instruction, because many find games to be a compelling experience.

Many users do not understand why good passwords and password management are important for information systems. This effort developed a scenario for CyberCIEGE to teach players about issues involved when developing a password policy for a computer system. Limited testing showed the scenario accomplishes this. CyberCIEGE uses a Scenario Definition Language to provide developers and educators the ability to create scenarios that focus on particular concepts. To streamline scenario development, a Scenario Definition Tool has been created. As a part of scenario development, this work also involved beta testing of the Scenario Definition Tool, a program that aids scenario developers in the creation of scenarios for the game. This testing resulted in several improvements to the tool.

14. SUBJECT TERMS Information assurance, CyberCIEGE, Scenario Definition File, Training, Password, Authentication			**15. NUMBER OF PAGES** 116
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

AUTHENTICATION SCENARIO FOR CYBERCIEGE

David S. Mueller
Civilian, Federal CyberCorps
B.S., University of California at San Diego, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: David S. Mueller

Approved by: Cynthia E. Irvine
Thesis Co-Advisor

Paul C. Clark
Thesis Co-Advisor

Michael F. Thompson
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Frequent media reports of the loss or compromise of data stored on computer systems indicate that attempts to educate users on proper computer security policies and procedures seem to be ineffective. In an effort to provide a means of education that will more fully engage users, the CyberCIEGE game was created. It is hoped that by playing CyberCIEGE users will absorb computer security concepts better than they have through more traditional forms of instruction, because many find games to be a compelling experience.

Many users do not understand why good passwords and password management are important for information systems. This effort developed a scenario for CyberCIEGE to teach players about issues involved when developing a password policy for a computer system. Limited testing showed the scenario accomplishes this. CyberCIEGE uses a Scenario Definition Language to provide developers and educators the ability to create scenarios that focus on particular concepts. To streamline scenario development, a Scenario Definition Tool has been created. As a part of scenario development, this work also involved beta testing of the Scenario Definition Tool, a program that aids scenario developers in the creation of scenarios for the game. This testing resulted in several improvements to the tool.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my thanks and appreciation to several individuals, without whom this thesis would not have been possible.

I would like to thank my advisor team of Dr. Cynthia Irvine, Paul Clark, and Mike Thompson, whose suggestions and feedback during both the scenario development and writing process proved invaluable.

I would like to thank Ben Cone, Carrie Ruppar, Chee Mun Ng, and Nai Kwan Tan, for taking the time to play and test the scenario, providing feedback and helping to validate that the scenario actually did what it aimed to do.

I would like to thank Daniel Warren and William Murray, whose courses gave me the educational knowledge presented in the scenario.

Finally, I'd like to thank Tanya Raven, Peter Denning, Gary Kreeger, Owens Walker, Jean Brennan, Deborah Shifflet, and the rest of the faculty and staff in the NPS Computer Science department for providing a wonderful and supportive educational environment.

This material is based upon work supported by the National Science Foundation under Grant No. DUE-0210762. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

A. THESIS STATEMENT

The purpose of this research was to develop a scenario for the CyberCIEGE game to train and educate users, system administrators, and computer security students in issues related to authentication and password policies. A secondary goal of this research was to perform beta testing of the CyberCIEGE Scenario Definition Tool.

B. THESIS SCOPE AND LAYOUT

This thesis describes the development of a scenario for the CyberCIEGE game to educate users in issues related to authentication and password policies. It also describes beta testing of the CyberCIEGE Scenario Definition Tool.

The thesis chapters are laid out as follows:

- Chapter I – Introduction and Background – This chapter introduces the project and provides a background discussion of the issues that motivate this thesis.
- Chapter II – Development Methodology and Scenario Discussion – This chapter describes the scenario that was developed and the process by which it was developed.
- Chapter III – Scenario Definition Tool Beta Test – This chapter discusses how the CyberCIEGE Scenario Definition Tool was tested and how the use of the tool affected the thesis. It also provides a more systematic test plan based on the testing experience.
- Chapter IV – Conclusion – This chapter provides a summary of the project and gives suggestions for related future work.

C. PASSWORD POLICIES

A computer system's user authentication process, sometimes called the Identification and Authentication (I&A) process, supports a policy to protect the information stored on the system. By allowing actions to be linked to the user that performs them, user authentication allows a system to provide such features as discretionary and mandatory access control, accountability, and auditing. Because of the importance of a reliable system-level access control mechanism, this thesis focused on the impact of password policies on system-level access control.

A system-level access control mechanism restricts access to a computer system to authorized individuals by requiring the user to provide the computer with a shared secret—the password—that ideally is known only by the user and by the computer system. Within the computer, a user is known by his or her user name. The user name alone is not sufficient to prove identity, since user names on a computer system are often well known [Kurzban 1985]. For example, the user names on many computer systems are part of the user's e-mail address, which is included in every e-mail message sent by the user, and is often made publicly available so that others can send the user a message. Since user names are well known, a computer system that required only a user name to gain access to the system would allow anyone who knew the user name to log in and pose as that user. So a second piece of information is needed in addition to the user name in order to control access to a computer system. Passwords allow users to prove their identities to the computer system.

1. Three Possibilities

User authentication schemes can be based either on secrecy or on unforgeability [Saltzer 1975]. Secrecy is based on a piece of information known only to the user and to the system. Unforgeability is based on the user's possession of something that is difficult to forge, and can be either a physical object or a unique physical characteristic of the user.

Fingerprints and retina images are common examples of unique physical characteristics that can be used to authenticate a user. While these can be attractive in that they are often hard to duplicate and cannot be easily lost, they are subject to variability (such as dirt on a finger) that forces a margin of error to be permitted, which can increase the rate of false positive matches. In addition, the equipment required can be expensive and is not found on many computer systems.

A second possibility is that a user can maintain possession of an unforgeable physical object, such that the system will authenticate anyone who can show possession of the object. The attraction of this option is that, like the first, is that it does not require a user to memorize something. However, the object can be subject to loss or theft, and thus is generally insufficient to be used on its own. It may also preclude remote access to a computer system from an arbitrary location, since a physical device is usually needed to

interface the object and the computer. Within a particular organization, this can be a viable option, since the organization can ensure that all workstations are equipped with the appropriate device.

The final possibility is the use of a piece of secret information. Ideally, this information is known only to the user and to the computer system. A password is a common means of implementing this mechanism. Since keyboards are standard equipment on computer systems, passwords can be easily entered and then transmitted over a network, permitting remote login from an arbitrary location. Simple theft or loss cannot occur, however coercive or subversive means can still be used to obtain a user's password. In addition, because of the finite (and in Western languages, relatively small) set of characters used, it is possible that hostile users using a systematic attack can determine the password. All of the possibilities are tried until one that works is found. This method is known as a brute force attack. Such an attack can be carried out either by a *direct brute force* attack, where the attacker makes repeated attempts to log in to a system, or by a *password cracking* attack, where the attacker obtains a password's encrypted form as stored on a system or transmitted over a network, then using a program on the attacker's own system to attempt to determine the password by encrypting possible passwords until one is found that matches the target encrypted password [Bishop 1995]. In order to decrease the effectiveness of a password attack, the organization responsible for maintaining a computer system must define an appropriate password policy. Password-based authentication systems also depend on the user to memorize the passwords. If the password is forgotten, the user becomes unable to access the system. User mistakes when typing the password can also prevent access.

It is also possible to combine these possibilities to create a multi-factor authentication system. One common example of this system is the bank Automated Teller Machine, where the user must supply both a physical object, an ATM card, as well as a piece of information, a personal identification number, in order to perform a transaction. Multi-factor authentication protects the card from malicious use in the event it is lost or stolen, since the malicious user does not know the personal identification number [O'Gorman 2003].

2. Elements of a Password Policy

There are several elements of a password policy that affect the effectiveness of a hostile user's brute force attack on passwords. Among these are the password length, character complexity or alphabet size, and change frequency, as well as lockout or delay policies associated with the authentication process. The number of possible passwords P for a given length L and alphabet size N is $P = N^L$. For a range of lengths from L_{min} to L_{max}, the number of possible passwords P is:

$$P = \sum_{i=L_{\min}}^{L_{\max}} N^i$$

One of the simplest methods of decreasing the effectiveness of a hostile user's attempt to discover an authorized user's password is by increasing the length of the password. Each additional character in length exponentially increases the number of possibilities to be tried, as seen in Table 1 below, where each row represents a different password length.

Another element of a password policy is the complexity of the character set or size of the alphabet allowed in a password. If an English language computer system only allows upper-case letters, or does not distinguish between lower-case and upper-case, then the passwords would only be made up of 26 possible characters. If the system does distinguish and permit both upper-case and lower-case, then the number of possibilities is raised to 52. Allowing numbers and symbols raises the number of possibilities further. The number of possibilities that have to be tried for a given length is exponential; increasing the character complexity increases the base of the exponent, as shown in Table 1 below, where each column represents a different number of possible characters.

	Alphabet Size		
Length of Password	**26**	**52**	**93**
4	4.57×10^5	7.31×10^6	7.48×10^7
6	3.09×10^8	1.98×10^{10}	6.49×10^{11}
7	8.03×10^9	1.02×10^{12}	6.01×10^{13}
8	2.09×10^{11}	5.34×10^{13}	5.60×10^{15}
10	1.41×10^{14}	1.44×10^{17}	4.84×10^{19}

Table 1. **Number of possible passwords as a function of alphabet size and password length. From [Warren 2003]**

A further benefit can be realized by placing a lower limit on the character complexity of a password. People have a tendency to use words in their language as a password, however a list of words for a given language already exists: a dictionary. Thus, rather than trying all possible combinations of characters, an attacker will often try working through a dictionary or list of words. Adding requirements that users mix the case of their letters or use numbers or symbols in their passwords helps to reduce the probability that this simple dictionary-based attack is successful, since it reduces the probability that the password is in the dictionary.

Allowing a range of password lengths increases the number of possibilities to be tried. If an organization requires passwords of exactly seven characters, then the attacker will only need to try passwords with seven characters. However if either seven or eight character passwords are allowed, then in addition to all of the seven character passwords, all of the eight character passwords will need to be tried.

In the past, limitations of the algorithm that produced the “encrypted” password for safe storage limited the length of the password, but present algorithms have practically removed length restrictions. However, human memory can limit the length of a password a user can remember, thus the concept of a pass-phrase came into being

[Kurzban 1985]. Rather than remember a sequence of characters, a user remembers a sequence of words. This has the result of generating much longer passwords that are still possible to memorize.

Requiring the user to change their password on a regular basis is intended to reduce the risk associated with an undetected compromise of a user's password [NIST 1985]. In the event a compromise is suspected, the password should be changed immediately. Requiring that a password be changed even when no compromise is suspected restricts the amount of time that a password that has been unknowingly compromised can be used, and the longer the period of time that a password is in use increases the chances that someone other than the password's owner learns it [Shinder 2003]. While a password change policy does not impact the time it takes an attacker to determine a password using a brute force attack, the time it takes to complete one means that by the time the attacker has successfully determined the password, there is a high probability that it will have been changed and will no longer allow access to the targeted computer system.

Related to the requirement that users change their passwords is the capability for a system to remember a user's previous passwords in order to prevent them from reusing a password. Users can also be required to keep a password for a minimum length of time. These two capabilities are often used together to prevent a user from changing his or her password, then immediately changing it back to what it was previously, effectively circumventing the requirement to change the password [Bickel 2003].

Perhaps the most effective method of preventing a direct brute force attack where the attacker is making repeated attempts to log in is a lockout policy. A lockout policy causes an account to be locked out, preventing any logins, after a certain number of sequential unsuccessful login attempts. In order to log in again, the user generally will have to contact a system administrator to have the account unlocked. Alternatively, the system can be configured to unlock the account automatically after a certain period has passed. With a lockout policy in place, a direct brute force attack becomes impractical, since after trying just a few passwords, any attempt to log in will fail.

While a lockout policy can be effective in preventing a direct brute force attack from being successful, it can also be used by the attacker to create a denial of service attack on the system, since locking out the account also prevents the legitimate user from being able to log in until the account is unlocked by a system administrator [O'Gorman 2003]. Because of this problem, some organizations may find it preferable to automatically unlock the account, rather than requiring a system administrator to unlock it.

An alternative to a lockout policy is a delay policy, where the system will wait a certain amount of time before allowing another login attempt after a failed login. Whereas a lockout policy disables the account that the user is attempting to log in to, a delay policy simply stalls the workstation for a few moments before another log in attempt can be made. This severely reduces the speed at which an attacker can make login attempts, making this kind of direct brute force attack impractical, and has the additional benefit of preventing an attacker from being able to cause a denial of service to the legitimate user. Table 2 shows how much time is added to a direct brute force attack of one million password possibilities when a system enforces various delay times between login attempts. The times listed in the table do not include the time required for the system to determine whether or not a password is correct or the time it takes an attacker, whether manual or automated, to transmit the next password. As the table shows, small increases in the delay time can have a significant impact on the time required to complete a direct brute force attack. The relationship between the two times is linear.

Delay Time (seconds)	Time Added
1	278 hours (11.6 days)
5	1389 hours (57.9 days)
10	2778 hours (115.7 days)
30	8333 hours (347.2 days)

Table 2. **Time added to a direct brute force attack of one million password possibilities given various delay times.**

One variant on a delay policy is to use increasing delays with each failed login attempt. This method has the advantage of not causing a long delay if the legitimate user makes a mistake on their first attempts to login, while an attacker would encounter an increasing delay on each attempt.

At first, it may seem that with a lockout policy, it is not necessary to place any restrictions on the password, since after just a couple of attempts the attacker would be unable to proceed further. However, lockout policies are effective only for attacks where the attacker is attempting to log in to the system. If the attacker can obtain the "encrypted" form of the password and perform a password cracking attack, additional factors such as password length and alphabet size are required to reduce the risk of a successful attack.

3. Summary of the Elements of a Strong Password

There is little agreement on what makes a strong password. When creating a strong password, the goal is to create a password that is difficult for an attacker to guess. Typical rules for creating a strong password include using a password at least eight characters long, with both letters and numbers, and doesn't include a dictionary word or other term that would be associated with the user, such as a name, birth date, or social security number [Sonnenberg 2003]. A system enforcing a strong password policy will often also include a lockout or delay mechanism.

4. Password Generation Mechanisms

Computer system passwords can be generated by either the computer or by the user. The terms *machine-generated* and *user-generated* are often used to describe which is used to generate a password. Machine-generated passwords are generated by the computer system and assigned to the user. User generated passwords are created by the user and entered into the system.

Machine-generated random passwords are considered to be more secure since the algorithm that generates them can ensure the password meets the defined policy. However, they can be more difficult for the user to remember, thus user-generated passwords are often attractive [Bishop 1991]. One variation is to have the machine generate a random password using pronunciation rules, generating a random password that can be pronounced, rather than using a simple random character generator.

Pronounceable random passwords are generally assumed to be easier to memorize than truly random passwords [Ganesan 1994]. Another variation is for the machine to generate a list of random passwords, and allow the user to select a password from that list. Often, user-generated passwords must conform to a policy that the computer can enforce, rejecting passwords that do not meet the policy.

5. Identifying an Attack

Reviewing system logs plays a major role in determining that a computer system is under attack [NIST 1995]. A system administrator can do this manually by visually reviewing the logs. While this may be a viable approach for a very small organization, most organizations would find this to be a poor use of the administrator's time, and would instead invest in an automated system that reviews the system logs and alerts the administrator when unusual activity is detected.

For the case of a direct brute force password attack, a system log would show a series of failed remote login attempts. For a password cracking attack, the system logs would not show any evidence that one is in progress. However, they may contain evidence that an "encrypted" password has been compromised, such as attempts to access the file storing the "encrypted" passwords or user logins from unusual locations outside of normal business hours.

6. User Resistance

Many users dislike passwords, and especially dislike having the complicated passwords that are the foundation for a strong password, but can be hard to remember. The cost to an organization in lost productivity when users forget their passwords can be high. Some estimate that 40% of IT help desk calls are password related, usually either because users have forgotten their passwords or have been locked out of their accounts [Bown 2004].

There are several reasons users tend to resist password policies. Users often cite difficulties with password enforcement mechanisms as reasons for their resistance. Requirements to maintain different passwords for different systems and policies that require frequent password changes are often cited difficulties. Adams and Sasse noted that users' knowledge of what makes a secure password was inadequate. As a result, users create their own rules for password design that, while the user may perceive them to

be secure, are not. Computer security departments often operate on a security-through-obscurity basis, on the assumption that the more that is known about a security mechanism, the more vulnerable it is to attack. As a result they tell the users, whom they perceive as "inherently insecure", as little as possible. Users tend to be security-conscious when they perceive the need for secure behavior, but, due to a lack of education and knowledge, often do not perceive such a need [Adams 1999].

As a result of this lack of knowledge, users often take actions that reduce the security of the organization's computer systems. Some write down their passwords. Others use similar passwords for different systems when differing requirements prevent reusing the same password.

A major goal of this research was to provide a tool that can help users understand password policy issues. It is hoped that with a better understanding, users will take their organization's policy more seriously and make an effort to comply with both the letter and the spirit of the policy.

D. MORE SOPHISTICATED ATTACKS

The attack that is presented in the CyberCIEGE scenario developed as part of this research is a direct brute force attack. Realistically, only an unsophisticated attacker would attempt this type of attack, which was selected for its simplicity and to prevent the player from being distracted by the complexities of more sophisticated attacks.

A more sophisticated attacker would be more likely to attempt to gain access to the system by some other means, such as looking for an exploitable vulnerability in an application, and then attempting to locate the file with the "encrypted" passwords and copy it for offline cracking, or would attempt to obtain the password by capturing it as it travels across the network. In the first case, once the attacker has obtained the "encrypted" password, the attacker can attempt to "crack" the password using his or her own computing resources. Tools that perform password cracking attacks generally start with a dictionary attack before attempting a brute force attack, as dictionary attacks have historically proven to be effective [Yan 2001]. The use of encryption protocols like Secure Shell [Loshin 2001], Transport Layer Security [Dierks 1999], and Virtual Private Networks [Ferguson 1998] make intercepting the "encrypted" password more difficult,

since the communication must first be decrypted before the "encrypted" password can be obtained. In addition, most systems are now storing "encrypted" passwords in such a way that only system administrators can access them [Feldmeier 1990]. A far more sophisticated attacker might ignore passwords entirely, instead installing a rootkit to maintain access to a compromised system [Levine 2004]. As discussed in Chapter IV, future work related to the scenario developed for this research could include adapting it to a different style of attack.

E. CYBERCIEGE

CyberCIEGE is a simulation game for the Microsoft Windows platform that places the player in the role of Information Technology Manager for an organization. The game is designed to teach key information assurance concepts and practices, and is extensible to allow developers to create scenarios targeted to specific audiences and topics. A game-specific Scenario Definition Language is used to create scenarios. Generally, the player is required to make choices regarding physical, technical, and procedural security to defend the assets of the simulated organization from attackers [Irvine 2005].

The game is based around a three-dimensional overhead view of the office of the organization under the player's control. Additional screens provide the player with the tools to define and configure the organization's IT infrastructure, which includes computers, networks, and other network-related equipment. The organization contains virtual users who use the infrastructure to meet their goals. If a virtual user cannot meet his or her goals, his or her productivity decreases, causing the organization to lose money. Zones can be used to restrict the movement of virtual users around the office, placing different requirements for access on different portions of the office.

In addition to supporting users who need to meet goals, the infrastructure also needs to protect the assets of the organization. Assets are stored on computers, and if they are not sufficiently protected, motivated attackers will compromise them. Assets have a motive value assigned to them, providing a mechanism for the scenario developer to define how far an attacker will go in order to compromise the asset. The higher an asset's motive value, the more sophisticated an attacker's methods become, requiring the player to deploy more thorough, and potentially more expensive, defenses to protect the

asset. Assets also have a cost associated with them, indicating the loss the organization incurs if the asset is compromised. Virtual user goals generally entail the reading and/or modification of assets.

Each scenario can be split into several phases, each with its own objectives that the player must complete before proceeding to the next phase. These phases provide a mechanism that can be used to represent changes over time, and to place events into a set sequence. Objectives can be defined in terms of goals achieved by virtual users or in terms of the player configuring components to enforce a particular security posture.

The game also includes conditions that are assessed during play, and triggers that cause a particular action to occur. When the set of conditions associated with a trigger is met, that action occurs. These triggers include actions such as winning or losing the game, progressing to the next phase, an attack on an asset, and the display of a message to the player.

Player motivation is provided by having player choices affect the user's budget. Productive virtual users make money for the organization and can increase the budget, while unproductive users and successful attacks lose money, decreasing the player's available funds. Making changes to policies, purchasing equipment, providing training to virtual users, and salaries for guards and IT staff all cost money, which is deducted from the budget, forcing the player to consider his or her options. Many scenarios cause the player to lose if the organization or player's budget runs out of money.

The elements described above are defined for the game using the Scenario Definition Language. Because it encompasses the wide variety of options available to scenario developers, the language is complex. To assist scenario developers in creating their scenarios, the CyberCIEGE Scenario Definition Tool was written [Johns 2004]. This application provides a forms-based interface to the Scenario Definition Language. It helps developers avoid syntactic errors when defining scenarios.

For this project, CyberCIEGE is used as a simulation platform to allow players to explore different possible password policies and what effect those policies could have on an organization.

F. THESIS QUESTION

Can a scenario for the CyberCIEGE game be constructed to train and educate users, system administrators, and computer security students in issues related to authentication and password policies?

G. SUMMARY

This chapter has provided an overview of the role passwords and password policies play in user authentication to computer systems. The next chapter describes the scenario that was developed to educate users about password policy issues.

THIS PAGE INTENTIONALLY LEFT BLANK

II. DEVELOPMENT METHODOLOGY AND SCENARIO DISCUSSION

This chapter will discuss how the CyberCIEGE game may be used to educate users on the authentication and password policy issues outlined in Chapter I.

A. REQUIREMENTS

The basic requirement was to develop an educational scenario to teach users about some of the issues involved in developing user authentication and password policies. It was an additional requirement that the scenario be enjoyable to the user as a game, and not be seen as a purely educational presentation. Users are less likely to become as engaged in an educational tool as they would be with something that feels like a game, as there is now virtually an entire generation of people who find games an immensely compelling and rewarding experience [Garris 2002].

The primary goal of the scenario was to teach the player the effects of password policy choices. In particular, it was desired to show that while problems can result from having weak policies, as most people would expect, issues could also arise from having a very strict policy. The scenario would focus on a low motive attack, as an attacker with a higher motive would likely start looking at other methods to achieve their goals, such as looking for application vulnerabilities or social engineering. An Internet connection is included, since many small businesses would likely consider it essential, even if the business case for Internet connection is not well grounded. The Internet connection will also facilitate the external attack. The value of user training as well as the role that the review of system logs plays in identifying intrusion attempts will also be addressed.

As scenario planning proceeded, it was determined that the design of the CyberCIEGE game would not permit a fully realistic simulation of password policies and procedures; in particular, the game does not offer the same level of granularity that a real system does. For example, in a real system an administrator is able to set exact values for minimum and maximum password length, whereas in the game there are only the options “short”, “medium”, and “long”. Furthermore, in most real systems password policy selections might have no discernable effect for long periods of time. But to keep the player’s attention and make the desired points, the game must provide quick feedback to

player choices, and as a result the impact of the player's choices is felt almost immediately. Therefore the scenario is a low fidelity simulation: Rather than providing an exact reproduction of the options a system administrator might have to work with, as would be the case in a high fidelity simulation, abstractions were made to emphasize the concepts most related to authentication [Prensky 2001].

The CyberCIEGE game provides three different configuration options related to password configuration that the player is able to set: Password length, complexity of the character set, and change frequency. These options are shown in Figures 1 and 2. For password length, the player can select between "short", "medium", and "long". The player also has the ability to select none of these options, which represents a choice of not requiring a password. For the complexity requirement, the player can select "any", meaning there is no complexity requirement, or "moderate" or "complex", with increasing complexity requirements. Increasing complexity means more use of mixed case letters, numbers, and non-alphanumeric symbols. For password change frequency, the player is able to select from "2 months", "6 months", "1 year", or "never". This setting controls the time interval between the computer requiring users to change their passwords. In addition to these items, the game also has procedural settings to indicate whether or not users are allowed to write down their passwords.

It was also determined that the scenario should not function in a "sudden death" manner where the player loses the moment an incorrect choice is made. Instead, the player should be allowed time to try different configurations to determine which ones are appropriate for the situation. However, failure to determine an appropriate configuration within a predetermined time will cause the player to lose.

In order to simplify the scenario and better control the player's experience, it was decided to structure the scenario so that the built-in attacks would not be used. Instead, attacks were developed using conditions and triggers. The capability for the scenario developer to selectively enable the game engine's built-in attacks was not a feature of the underlying simulation engine until the scenario was well into development.

Feedback while the scenario is being played takes two different forms. Popup messages provide a narrative description of the events of the game as they progress,

while monetary bonuses and penalties are given as the player meets the goals of the game or allow negative events to occur, respectively.

B. DESCRIPTION OF DEVELOPED SCENARIO

The developed scenario is set in a fictional retail business that comes under a cyber attack from a competitor. In the role of IT administrator, it is the player's job to configure the company's computers in a manner that will fend off the attack.

1. Scenario Overview

As the scenario starts, Tom's Tools has just hired the player as their new IT administrator. In the first of the scenario's two phases, the player needs to configure the password settings on two machines: the workstations used by the virtual users Tom, the owner of the store, and Jane, who handles most of the sales and customer contact tasks at the store. These settings are currently the focus of attention, as system logs show numerous unsuccessful attempts to remotely log into their workstations.

Because the store is small, with very few employees, remote access must be enabled so that the staff members are able to access their data and perform work even while away from the store. In addition to their brick and mortar store presence, Tom's Tools also sells online, thus the web site and mail server, hosted off site at a web hosting facility, needs to be accessible from the store workstations.

Once an acceptable password configuration is reached, the scenario moves into its second phase. The attacks are determined to be coming from Hammer House, a competitor, and are targeting the store's computer inventory, stored on a server on-site and accessible from both Tom's and Jane's workstations. With this information, it is determined that the attacks need to be taken seriously and that the organization needs to move to a higher level of security—in this case, setting password requirements to their highest settings.

Once the player passes the second phase, the game finishes.

2. Scenario Walkthrough

When the game starts, the workstations are set at minimum default configurations. If the settings remain too low, the attackers will be able to successfully penetrate the system, causing the store to lose money. Since Jane's access to the inventory is limited to

viewing the inventory and changing the quantity of items in stock as a result of sales and returns, compromising her computer has a lower cost than compromising Tom's, which has the additional capabilities of adding and removing items from inventory as well as changing prices.

If the password settings are set too high, Tom and Jane will forget their passwords and a small cost will be incurred, representing the need for the system administrator to reset a password. If the configuration option allowing passwords to be written down is set, Tom and Jane may write them down to avoid forgetting them; however, non-employees in the store, such as customers, might see the written passwords, which will lead to a compromise of the inventory.

For the first phase, an acceptable password setting is any combination of password length, complexity, and change frequency with the exception of all settings at their lowest or highest. An example of an acceptable password setting to pass the first phase, shown in Figure 1, is "medium" password length, "moderate" character set complexity, and passwords must be changed every six months.

Figure 1. Example password settings to pass the first phase.

When the second phase is reached, the environment under which the company is operating has changed, thus the security settings need to change. In this case, the password length, complexity, and change frequency all need to be set at their highest settings, and writing down passwords needs to be forbidden. If the user fails to adjust the password settings, the attackers will eventually succeed, causing the player to lose. In order to avoid the problems of users forgetting their passwords, additional training will have to be purchased. The reason for this is that with the training, the users will have a better understanding of the security issues involved, and thus will make more of an effort to remember more complicated passwords [Adams 1999]. The password settings required to pass the second phase, shown in Figure 2, are "long" password length, "complex" character set complexity, and passwords must be changed every two months.

Figure 2. Example password settings to pass the second phase.

3. Relationship to Real World Concepts

The first phase of the scenario is meant to represent a typical security situation, where the needs for computer security must be balanced against the willingness and ability of employees without significant computer security training to comply with computer security policies.

The second phase is meant to represent a situation where the security requirements of the situation exceed the user's ability to comply with them. When that happens, the user becomes the weak link in the chain, and "fixing" users is not something a system administrator can do with a few clicks of a mouse. Instead, the users have to be trained. Although expensive, training is necessary for the organization to succeed.

The individual settings that the player must select, in particular during the second phase, are not intended to convey exact settings that the user should copy verbatim to real-world systems. Rather, they are meant to convey the general security posture of the organization at the time. In the first phase, the appropriate posture is one where the settings are neither too weak nor too strong. The second phase is meant to convey a change in the environment that requires a move to a high security posture. In particular, this abstraction is seen in the setting for password change frequency which would, in reality, have little effect for a temporary change in the organization's security posture that spans a period of hours to days, as portrayed in the scenario. However, if this change were to span a period of months or years, then increasing the password change frequency might be a relevant step to take.

As a result of this, the exact meanings of the relative terms used for the password settings, in particular "short", "medium", and "long" for password length and "any", "moderate", and "complex" for character complexity are not important. Rather, it is the impact that these differences have on security that is emphasized. The decision to use these relative terms was made on the basis of ease of presentation and to allow their exact meanings to be left open for the scenario developer to determine [Thompson 2005]. For this scenario, it is not necessary to assign an exact meaning.

Nevertheless, it may be constructive to give examples of what might be considered reasonable interpretations for these definitions at the time of writing. For password length, "short" might mean a password at least four characters long, "medium" might mean at least seven characters long, and "long" might mean more than at least ten characters long. For character complexity, "any" means that there is no restrictions placed on the password, "moderate" might mean that the password cannot be a name or

dictionary word, and “complex” might require the use of both upper and lower case letters along with at least one number and one non-alphanumeric symbol.

As the scenario attempts to convey, the definition of what is a reasonable password policy depends on the risks and threats that face an organization. An attacker with a high motivation to break into a system will apply more time, effort, and resources to doing so. A small retail organization like the one depicted in the scenario is not likely to hold much interest for most attackers, thus the organization does not face a high threat. For this type of organization, a moderate password policy of requiring at least seven character passwords that are not dictionary words and are changed every six months is likely to be sufficient.

C. SCENARIO TESTING

Initial testing of the scenario was performed during development and by one of the advisors. Upon completion of the scenario, students who were also working on CyberCIEGE were invited to test the scenario by playing it and providing feedback.

1. Testing During Development

Development of the scenario was iterative, where a few elements of the scenario were created, then built and run to ensure that they functioned as desired. The process was repeated as more elements were incorporated. Occasionally, previously created elements would have to be changed and then retested, either due to changing requirements in the developing scenario or due to changes in the CyberCIEGE game, which was still evolving as scenario development progressed.

During this phase, testing was performed by playing the scenario and visually verifying that the desired functionality was present. For example, at one point scrolling messages were added to the ticker at the bottom of the screen to help convey the image of an active retail store. Once the messages were added, the game was run without player interference and the messages were observed.

2. User Testing

Once scenario development was complete, it was installed on a server that provided the CyberCIEGE game on a shared folder. Students involved in the CyberCIEGE project were then invited to play the scenario and provide feedback. Copies of the player evaluations are attached in Appendix B. The CyberCIEGE

Campaign Analyzer was also used for an objective assessment of how the testers played the scenario.

Overall, users seemed to grasp the basic concept of the scenario: that it was attempting to explore issues related to the creation of a password policy and individual passwords. Users seemed to think the educational aspects were there, though some felt more instruction was needed. As to whether or not it was enjoyable as a game, there were mixed reactions, with users indicating that more direction to the player was needed. Users also reported that it was possible to pass the first phase by configuring only Jane's workstation, which is not what the scenario intended. There were also reports of a crash when the "Zone" tab in the game was selected; this problem was traced to a configuration file that was missing when the scenario was installed on the server.

Of the five games played, two were played to completion. In both cases, the player lost. In once case, the player ran out of money, and in the second, the player did not make all of the necessary configuration changes, and as a result fell victim to a successful attempt by the attackers to modify the store's inventory. In the other three sessions, the players terminated the game before it was complete. In two of these cases, the player quit while in the second phase, once after the attackers were able to read the store inventory, an event with a high cost but not normally resulting in immediate loss. In the final case, the player quit the game while still in the first phase.

D. SUMMARY

The result of this process was the creation of a scenario that gives the player insight into some of the issues involved when crafting a password policy. It is intended that this scenario become part of a larger collection of scenarios to complement an introductory computer security course or other overview of computer security issues. Additionally, this scenario was the first to be developed from the outset using the CyberCIEGE Scenario Definition Tool [Johns 2004]; a discussion of this process follows in the next chapter.

III. SCENARIO DEFINITION TOOL BETA TEST

The CyberCIEGE game includes a robust text-based Scenario Definition Language that is used to create scenarios [Irvine 2004]. However, with this robustness comes complexity, and complexity can make it difficult for people to write scenarios for the game [Johns 2004]. A program that runs under Microsoft Windows, commonly referred to as the Scenario Definition Tool or SDT, was designed and implemented that provides a point-and-click forms-based interface for the creation of scenarios. The scenario implemented in conjunction with this thesis was among the first to be created with the SDT. In addition, it involved a person who did not have significant experience in scenario creation by direct manipulation of the raw Scenario Definition Language.

A. HOW THE SDT WAS USED AND TESTED

Formal testing and verification of the SDT was not conducted for this thesis. Rather, the tool was used to develop the scenario, with correct functioning of the scenario in CyberCIEGE used as an indication that the SDT was properly generating the scenario. The testing model is most closely compared to the commercial software concept of a beta test, where software close to the final product is provided to users to test it in real conditions [Neff 2003]. As a result, testing of the SDT was performed as part of the same iterative testing cycles that were used to test the scenario itself. When a problem was uncovered, it was reported to the SDT developers, and when a new version intended to resolve the problem was released, it was tested to verify that the tool exhibited improved functionality.

In particular, testing of the SDT was focused on finding problems in three major areas: interface, consistency, and proper scenario generation.

1. Interface Testing

Interface testing was intended to test the visual and user interaction elements of the SDT. This covered the basic usability and usefulness of the tool. Usability is an indication of how the system interacts with the user [Ferré 2001]. Usefulness is how a system enhances the ability of a user to complete a task [Davis 1989].

Specific aspects of the SDT that were checked for usability and usefulness included any commands or sequence of commands that would cause the tool to crash, clarity of user interface elements and how they functioned, and consistency in user interface design. Each of these will be discussed below.

The overall stability of the tool seemed good. There was one case where the tool could be caused to crash on a regular basis, as detailed in the following section. Early versions of the tool did contain user interface elements, such as menu commands, for functionality that was not yet fully implemented, but there was no built-in indication that this was the case other than selecting the command and observing that nothing happened. As these functions were implemented, this ceased to be an issue.

The clarity of the user interface elements was another area that was examined through testing. In this area the tool did have some shortcomings. In particular, the design tended to assume the developer was familiar with the syntax of the scenario definition language, as there were several places that did not give any indication of what the appropriate input values were. Having a copy of the scenario definition language [Rivermind 2004] was helpful. To remedy this problem, a help menu entry to display the language specification was added to the SDT. A basic developer's guide has since been written which provides an overview of the tool, which is a helpful addition to the separate language specification [CISR 2005].

The final major area addressed by interface testing was consistency in the user interface. Overall consistency within the tool was good, but it does fall short of meeting published user interface guidelines for Windows applications [Microsoft 2004]. In particular, there were problems with the use of checkboxes versus radio buttons as described below. Additionally, guidelines regarding the format of menu items had not been followed, namely the use of ellipsis after the name of a menu item that will present a dialog box for further user interaction before the command is completed, and disabled menu items in certain contexts.

2. Consistency Testing

Consistency testing was primarily concerned with evaluating whether or not the SDT properly saves and restores developer-supplied data. The scenario was developed

over many different sessions. Closing the scenario and then opening it later and finding it the same as it was before indicated that the SDT was properly saving and restoring its own state. Several versions of the SDT operated on the same scenario data without loss, and the directory containing the data was transportable between different computers running the SDT. No major issues in these areas were found.

3. Proper Scenario Generation

Testing for proper scenario generation was used to determine if the SDT was generating valid, playable scenario definition files. The code for these files was generated primarily from fixed code associated with the various objects included in the scenario, with various portions supplied in developer-entered fields.

The fixed code did not generate problems, however there were times when a fixed object depended on another object that was not present in the scenario. Earlier versions of the SDT that did not include any validation checking would generate an invalid scenario definition file. Later versions that included validation checking were able to check for missing dependencies and report them to the developer.

Developer-supplied text presented a more serious problem. Many of the fields were simple text boxes that gave no indication of the type and range of permitted values. A copy of the scenario definition language documentation [Rivermind 2004] was necessary in order to determine the appropriate values. As with the fixed code mentioned previously, the earlier versions of the SDT that did not include validation checking could generate invalid scenario definition files, while later versions included validation checking to guide the developer in correcting problems.

Problems with the scenario definition file can be caught in three places. Initially, there was no validation, and problems would either cause that element of the scenario definition file to be ignored or cause the game to crash. When the game crashed, a file named crash.txt was generated, and could be used to help diagnose the problem. Validation checking was later added in two locations: as part of the game itself, and in the SDT. Problems caught by in-game validation still cause the game to quit, with a file named parseErrors.txt generated to provide information about the cause of the problem.

Validation within the SDT can be run before the scenario definition file is generated, and can assist the developer in finding errors prior to game execution.

B. SDT ISSUES

Some of the issues uncovered during testing of the SDT and how these issues were responded to are described below.

1. Some File Menu Commands Do Not Function

It was discovered that the "Open Scenario" command in the "File" menu as well as the commands in the "New" submenu did not function. The "Open Scenario" command was repaired for the next revision of the SDT. The "New" submenu problem required more work, but a temporary workaround that consisted of right-clicking on the desired descriptor in the Reusable Sets Library section of the SDT window and selecting "New" from the pop-up menu was used until the problem was fixed.

2. Adherence to User Interface Guidelines

The SDT contained multiple violations of the published user interface guidelines for Windows applications [Microsoft 2004]. The Scenario Information screen on the SDT contained four radio buttons labeled "Use Small Office", "Use Work Office", "Internet", and "Static Network". Each option functioned as an individual on-off switch, and thus should be checkboxes instead of radio buttons, as radio buttons are used to select one from a set of mutually exclusive choices. The office-related buttons were ultimately changed to popup menus to allow scenario developers more flexibility in using different office configurations.

Several menu items, notably "Open Scenario", "Save As", and "Save Scenario As" in the "File" menu and "Import SDF", "Project Settings", and "Clone Project" in the "Tools" menu, present a dialog box for further developer input before the command can be executed. User interface guidelines call for the use of ellipsis at the end of the menu item in this situation, but the ellipses were not present.

There were situations where certain menu items do not apply. In particular, the "Save As" command does not apply if the Scenario tab is currently selected. In this case, and other cases where the current context precludes the use of a particular menu item, the menu item should be disabled so that the developer cannot select it.

3. "Save Scenario As" with Open Descriptors Causes Crash

When attempting to use the "Save Scenario As" command in the "File" menu to save a copy of the current scenario with a different name, the SDT would crash if there were any open descriptor tabs. A temporary workaround was to close the open tabs before saving. The problem was remedied in the next revision of the SDT.

4. Missing Scroll Bars on Text Boxes

Two text boxes that allow a significant amount of text to be entered were missing scroll bars, and, as a result, did not scroll beyond the displayed text area. The two boxes were the "Initial Briefing" text box on the Scenario tab and the "Message" text box on the Trigger tab for the Set Phase trigger class. These text boxes were corrected in the next revision of the SDT.

C. HOW THE SDT SUPPORTED SCENARIO DEVELOPMENT

The SDT was found to be an excellent aid in developing the scenario. While familiarity with the Scenario Definition Language was still needed to fully understand and utilize the features available in CyberCIEGE, using the SDT still provided substantial assistance. With the SDT, it was not necessary to know the exact syntax of the language; a familiarity with the various options was sufficient. As a result, less time was spent developing small scenarios to help learn the details of the language, allowing additional time to focus on development of the full scenario for this project.

When development of the scenario first began, the SDT had very limited ability to validate that the scenario being developed did not contain any errors or missing components. As a result, it could generate a scenario that would cause the CyberCIEGE game to crash, as the game has a limited tolerance for errors in the scenario definition file. As development of the SDT continued, the addition of validation features in the SDT and in the game proved to be valuable in improving and debugging the scenario.

D. SDT TEST PLAN

Although formal testing and verification of the SDT was not a part of this project, a test plan was developed, which has laid the groundwork for a more formal test. It is expected that future work will use this plan to develop complete test procedures for rigorous testing of the SDT. The purpose of this testing is to ensure that the SDT properly generates scenario definition files. The game can be assumed to properly

interpret scenario definition files. Either visual inspection of the generated files or execution of the scenario in the game can be used to verify correct scenario generation.

1. Test Plan Philosophy

The number of fields and elements in the SDT make exhaustive testing of every possible value and combination for each field infeasible. The beta test described earlier in this chapter indicates that the basic generation of scenarios appears to be correct. The focus of the testing should be on the items that have a major impact on a scenario, and areas that have not been extensively examined via beta testing. Previous testing had already validated that the CyberCIEGE game produces the expected results from a scenario definition file [LaMore 2004]. Test procedures developed from this plan should make clear the outcome that is expected from correct functioning of the SDT.

2. Menu Command Testing

The "File" menu contains the typical "New", "Open", "Close", "Save", and "Exit" commands. Each of these should be tested to ensure that the application behaves correctly. For example, if a change is saved, the scenario should then be closed and re-opened to ensure that the save was successful.

Commands in the "View" and "Help" menus bring up information in helper applications such as WordPad, Notepad, and Adobe Acrobat Reader. These commands should each be tested to ensure that the appropriate information is displayed.

The majority of testing should focus on the commands in the "Tools" menu. Testing for each command is described below.

a. Build

The "Build" command takes the current scenario and generates a Scenario Definition File (SDF) that the CyberCIEGE game executes. This function can be tested by loading or developing a scenario in the SDT, then building it and either running it in the game to see if it functions as expected, or by visual inspection of the generated SDF. The expected output generated by the Build command can be determined by comparing the SDF to the correct syntax of the language as defined in the Scenario Format Template (SFT) document [Rivermind 2004]. Testing of the Build command should demonstrate that all significant fields within the SDT are properly represented in the generated SDF.

b. Run

The "Run" command executes the CyberCIEGE game with the current scenario. It should be tested to ensure that it functions as expected.

c. Import SDF

The "Import SDF" command imports an SDF that was generated elsewhere and opens it in the SDT, allowing a developer to edit it. This command can be tested by playing a scenario and making various choices. The game should then be saved, which generates a new SDF. This SDF should then be imported into the SDT, which should then be used to build a new SDF, and this SDF should be visually compared to the one saved by the game.

d. Project Settings

The "Project Settings" command brings up a window that allows the developer to edit project-related settings. These are the directories in the file system where the project, CyberCIEGE game, and the user's preferred program for viewing text files are located. This should be tested to ensure that any changes made to project settings are properly applied.

e. Validate

The "Validate" command checks the current scenario for errors including invalid field values and missing dependencies. The SFT document should be examined to determine appropriate values for each field to be tested. Particular attention should be paid to border cases (values near the allowed minimum and maximum) and type mismatches, such as entering a string when a numeric value is required. The tester will expect the command to report errors when an inappropriate value is entered into a field, and not report an error when a value is correct.

f. Clone Project

The "Clone Project" command creates a copy of the existing project. This command should be tested by using it on an existing project, then comparing the two projects to verify that the original project and the copy are the same. A tool that can compare a file or set of files for differences, such as CSDiff [ComponentSoftware 2005], may be useful for this testing.

g. Validate / Build / Run

The "Validate / Build / Run" command is provided as a convenience to the developer. It first validates a scenario for correctness, then builds it, and finally runs it in the CyberCIEGE game. This command should be tested by first using it, and then separately executing each command to ensure they produce the same results.

3. Scenario Element Testing

Due to the number of fields included in the SDT, it is unlikely that resources will be available to test each one. The sections below detail specific elements that merit special attention, as they do not appear to have been used extensively to date. These tests should be performed as part of testing the "Build" and "Validate" functions described above.

Many of the fields can be tested by simple inspection in the game, by setting a value in a field and then running the game and visually verifying that the value is properly reflected. Where there is a set of checkboxes, each can be tested by setting all of the checkboxes to on, then running the game to note that all of the appropriate options are set. They can then be set to off, the game can be run again, and visually verified that they are no longer set.

a. Scenario Tab

The Scenario tab holds basic information that applies to the entire scenario. Much of the information on this tab is simply presented verbatim in the game, such as the briefing text. Areas that should be focused on are the Attack Masks section as well as the NonServerDefaultPublic, End on Compromise, Easy Training, Easy ACLs, Use Catalog, Networks Everywhere, and Guards Cost at Startup options.

b. Asset Tab

The Asset tab is used to define the assets in a scenario. Areas that should be focused on are the Access Control List and Cost List sections, by creating various entries in the Access Control and Costs Lists and ensuring that they are properly generated and reflected in the game.

c. Catalog Component Tab

The Catalog Component tab is used to define the hardware devices that are available for the player to purchase. The Configuration Settings section of this tab, used

to create the default settings for a component, should be focused on, and can be tested by using the all-on, all-off method described in section D.3.

d. Condition Tab

The Condition tab is used to define conditions that the game tests for during execution of a scenario. Only the AssignedComputerHas, UserTraining, ObjectiveCompleted, and PhaseCompleted conditions have been extensively tested. The other conditions require additional testing. These can be tested by creating one of each type of condition, then verifying by inspection of the generated scenario definition file that each condition was properly generated and matches the expected syntax as defined in the Scenario Format Template.

e. DAC Group Tab

The DAC Group tab is used to define the discretionary access control groups available in the scenario. It has just one element on it and does not require extensive testing.

f. Department Tab

The Department tab is used to define the employee departments available in the scenario. There are no elements on it other than the name of the department, so additional testing is not needed.

g. Filter Tab

The Filter tab is used to define firewall rules. This function is currently being tested as part of another thesis that focuses on the use of filters.

h. Goal Tab

The Goal tab is used to define the goals that can be assigned to virtual users in the scenario. The assignment of goals to specific virtual users is performed in the User tab of the SDT. While the SDT has been tested with relatively simple goals involving a single asset or Software element, testing of goals that entail several assets and different Software elements is needed. Additionally, the “Filtered Software” section needs to be tested. These can be tested by using the SDT to construct a goal with several assets, Software elements, and Filtered Software elements. The resulting scenario definition file should be visually inspected to determine whether or not the generated goal matches the expected syntax as described in the Scenario Format Template.

i. Integrity Tab

The Integrity tab is used to define the levels of integrity that can be applied to assets. It needs to be tested by creating various integrity levels and examining them in the Integrity section of the Security Labels window in the game.

j. Network Tab

The Network tab is used to define the networks available for the player to use to connect computer and other network components together. As networks are simply named wires, further testing is not needed.

k. Objective Tab

The Objective tab is used to define the objectives that the player will need to meet in order to win the game. This tab is fairly straightforward, but testing is needed to determine if an objective can span multiple phases. This is accomplished by creating such an objective, then visually inspecting the generated scenario definition file to determine whether or not the generated objective matches the expected syntax as described in the Scenario Format Template.

l. Component Network Connection Tab

The Component Network Connection tab is used to define the security properties associated with the connection of a network component to a network. This has not been extensively used and needs to be tested. The User Group World section can only be tested by inspection of the generated scenario definition file, since it is not currently used in the game. The Access Control List and MAC Connection Settings sections can be tested by creating entries and confirming their presence in the Network section of the Component tab in the game.

m. Procedural Settings Tab

The Procedural Settings tab is used to define the settings that are referenced by physical components and zones. These settings are used to configure components at the start of the game and are applied to any hardware purchased and placed within a zone. This has not been extensively used and needs to be tested. The Boolean Procedural Settings section can be tested by the all-on, all-off method described in section D.3. The other settings are ranges that can be tested by selecting various values and confirming their settings in the game.

n. Phase Tab

The Phase tab is used to define the different phases of a scenario. Each phase can contain different objectives that must be met before the phase can be completed. This tab is fairly straightforward and extensive testing is not needed.

o. Physical Component Tab

The Physical Component tab is used to define the hardware devices that are present when the scenario starts. While it has been used, the majority of the fields have not been used extensively and need to be tested. The checkboxes in the Configuration Settings section can be tested by the all-on, all-off method described in section D.3.

p. Secrecy Tab

The Secrecy tab is used to define the levels of secrecy that can be applied to assets. It needs to be tested by creating various secrecy levels and examining them in the Secrecy section of the Security Labels window in the game.

q. SupportStaff Tab

The SupportStaff tab is used to define virtual characters that perform security and IT support functions for virtual users. This has been used but some additional testing is needed. In particular, virtual characters with various attributes need to be tested by creating some support staff characters with various values. The resulting scenario definition file should be visually inspected to determine whether or not the generated virtual character matches the expected syntax as described in the Scenario Format Template.

r. Trigger Tab

The Trigger tab is used to define events that occur when a certain condition or set of conditions is met. It has been used, but it needs testing to ensure that the proper fields appear for each Trigger Class, and that the runsWhilePaused and Trigger Firing Condition Values work correctly as these are newer and are not well tested. Triggers can be tested by creating one of each type of trigger, then verifying by inspection of the generated scenario definition file that each trigger was properly generated and matches the expected syntax as described in the Scenario Format Template.

s. User Tab

The User tab is used to define the virtual users in the scenario. Because this option has been used a lot, the primary areas that should be checked are the Department, Secrecy, Cost, and Integrity Fields. These can be tested by setting various values and visually verifying that they are properly reflected in the User tab of the game.

t. Workspace Tab

The Workspace tab is used to define the positions that furniture and virtual users can be assigned to. This can be tested by creating various locations within a scenario, assigning users and furniture to them, and verifying their correct placement in the game. The Refresh button updates the User and Computer columns to show the placement of these objects in the current scenario, and can be tested by setting various user and component locations in their respective tabs, and then clicking the Refresh button to verify that it shows the correct placement. The Import button does not need to be tested further.

u. Zone Tab

The Zone tab is used to define the security zones for the scenario, and is closely associated with the Procedural Settings tab. Checkboxes can be tested by using the all-on, all-off method described in section D.3. Other fields can be tested by selecting various options in a scenario and visually confirming their settings in the game.

E. SUMMARY

The SDT proved to be an invaluable tool in creating the scenario. As development and testing progressed, bug fixes and feature additions improved the usefulness of the tool.

The test plan developed follows two general approaches to testing. Both involve creating scenario elements in the SDT, then checking to ensure the SDT properly generated the scenario. The first is by running the resulting scenario in the game, and visually verifying the correct values are present. This may be preferable since it also provides a check that the syntax of the scenario is correct. However, some items lead to more complicated behavior that may be difficult to predict. In this case, the scenario can be checked by visual inspection of the scenario definition file itself and comparing it to the Scenario Format Template's specification for the syntax of the element being tested.

IV. CONCLUSION

A. SUGGESTIONS FOR FUTURE WORK

As this project progressed, it became clear that there were several items that lend themselves to future work, not just in the scenario but also in the SDT and the CyberCIEGE game.

1. Scenario

There are several elements of the scenario that could use further improvement. These can be grouped broadly into three categories: feature enhancements, improving realism, and improving playability.

a. Feature Enhancements

During development of the scenario, new features were added to the CyberCIEGE game and to the scenario definition language. Time considerations prevented some of these features from being incorporated into the scenario. The pertinent features are discussed below.

Perhaps most critically, the game added the option for players to not require a password. The scenario should be updated to take this into account when evaluating the policies that the player has set. Specifically, conditions that test for the player having selected the option of not requiring a password need to be created. To support this, the triggers that check for various settings will need to include these conditions.

One new feature is balloon messages, where text appears connected to virtual users on the screen via cartoon-style speech balloons. Some of the messages that currently appear in the scenario as popup text messages could be converted to use these balloon messages. One possible candidate for this would be messages related to virtual users forgetting their passwords.

Another new feature is the ability for the scenario to alter the text that appears as a virtual user's thoughts in the sidebar of the Office tab. In the current scenario, these messages are being generated from the game engine, and were not paid attention to during scenario development. These game-generated thoughts could be

misleading to players as they may not reflect the direction the scenario's storyline takes, and the scenario should be updated to generate thoughts that are aligned with the plot. In the same vein, the scenario should alter virtual user happiness levels to reflect the events that occur in the game.

Finally, the capability for the scenario to provide a quiz to the player between phases was added. Since this is an education-oriented scenario, it may be appropriate to add some quiz questions to the scenario.

b. Improving Realism

The scenario is currently built around an attack strategy based on a direct brute force attack, which is unlikely to pose a serious threat to an organization since it can be easily prevented with an account lockout policy. Realism in the scenario could thus be improved by changing the attacker strategy; however, care would be needed in the design of a new attack strategy to ensure it does not distract the player from the educational goals of the scenario. There are a couple of different approaches that could be taken to developing a new attack strategy.

The first approach would be to redesign the scenario around a different, more sophisticated attack. Depending on the new attack, this may be as simple as changing some of the dialog presented to the player.

The other approach that could be taken would be to alter the scenario to take advantage of the attacks built into the game engine. In order for this to work, it would be necessary to ensure that the game engine contains attacks that are appropriate to the educational goals of the scenario, and that the scenario enables only those attacks.

There is also concern that the scenario could lead the player to make unrealistic conclusions about password policies, such as concluding that a password needs to be changed every two months. One possible way to address this would be to emphasize that the policy required to pass the second phase is an exceptional case, and not the normal case. Alternately, the scenario can be changed to require a more realistic password policy to complete phase two. For example, the change frequency for phase 1 and phase 2 could be the same, e.g., six months or a year. Password complexity could become the focus of the difference between phase 1 and phase 2, with "moderate"

implying a password not easily guessed, but potentially including a dictionary word. A "complex" password would exclude dictionary words. In the revised scenario, the student would be led to understand the risks of using dictionary words if the attacker has the means and the motive to obtain hashed password values.

c. Improving Playability

Playability issues were raised during user testing of the scenario. Some players expressed concern that they were unsure exactly what they were supposed to be doing, and noted that it was not clear that there were two distinct phases in the scenario that had different goals. Modifications to the scenario should be made to clarify these issues, but care should be taken to ensure that these modifications do not explicitly tell the player what to do. In particular, the descriptions of the objectives as provided in the game are terse, and could be expanded.

The game and scenario use relative terms for the options used in the password policy. However, there is nothing in the scenario to give the user an indication of what the relative values mean. The player might expect to find information about these options by bringing up the CyberCIEGE Encyclopedia pages for the component and zone tabs. While this information is in the encyclopedia, the player has to follow a link from the page that initially comes up and it does not add a lot of insight. Alternately a scenario-specific encyclopedia page could be displayed using a trigger. This would permit the password policy options to be defined in terms specific to this scenario.

Scenario development was performed by taking an existing scenario, removing unwanted components, and modifying and creating others to meet the goals of this project. There may still be excess elements that do not affect the scenario, and an analysis should be performed to verify if this is indeed the case, and strip out any excess elements that are identified.

2. Scenario Definition Tool

Testing of the SDT revealed various issues with the tool that needed to be corrected, as described in Chapter III. Some issues remain outstanding, in particular those related to the user interface. An effort to bring the SDT into conformance with Microsoft's user interface guidelines for Windows applications [Microsoft 2004] would improve overall usability.

Better integration with the scenario definition language would also be beneficial. A sidebar that gives a description for the option currently selected, including a range of appropriate values, could help build scenarios more quickly. An example of this behavior can be seen in the XMLSpy application from Altova, as shown in Figure 3 [Altova 2005]. Here, the left side of the window shows details about the "xmlns" attribute of the "html" tag, including the type of data that is allowed, and in this case, the exact value required by the XHTML 1.0 standard. One possible alternative to using a sidebar would be to provide a tool tip that displays additional information about a field when the user leaves the mouse pointing to it for a couple of seconds.

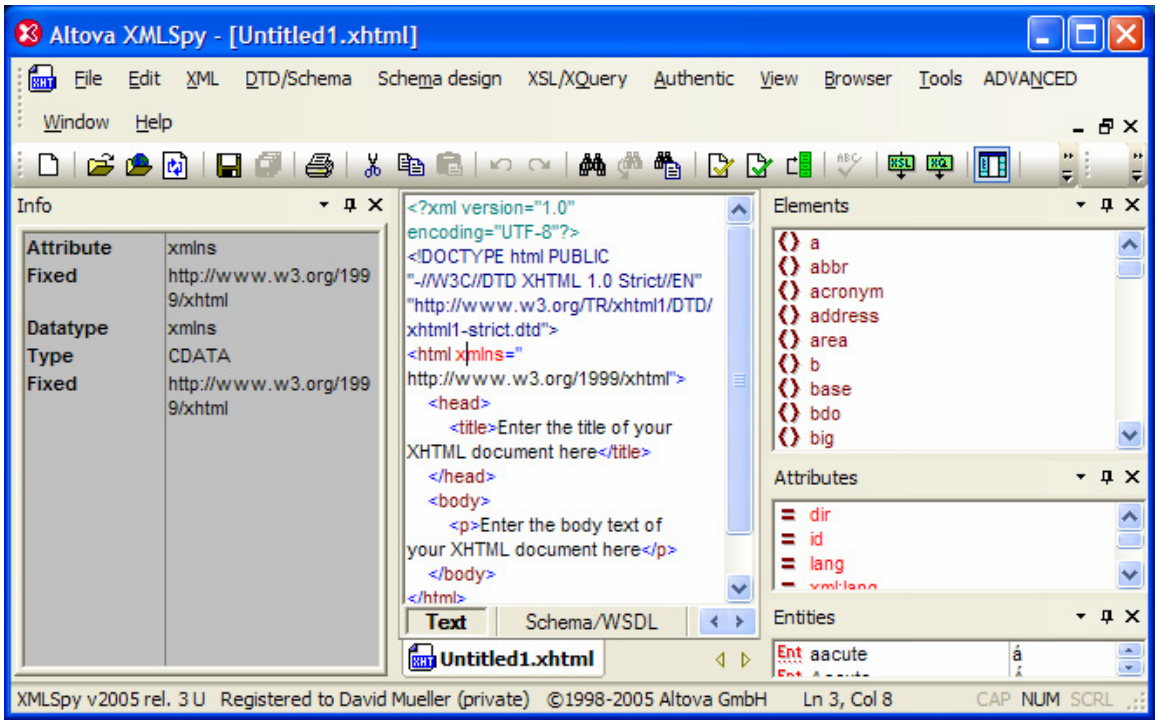

Figure 3. Altova XMLSpy gives information about the element currently being edited on the left side of the application window. [Altova 2005]

The list of elements in the trees for the Reusable Sets Library and Current Scenario are both the same, yet do not appear in the same order. For purposes of consistency they should both appear in the same order, preferably alphabetical order. In addition, the SupportStaff element uses mixed alphabetical case to denote the separate words, whereas other elements have a space included in the names. A space should be added to the SupportStaff element's name for consistency.

The SDT should be enhanced so that commands that do not currently apply cannot be selected. For example, the "Run" command should be disabled until after the scenario has been successfully built.

Many applications, web browsers in particular, have popularized the tabbed interface used in the SDT. Most of these tabbed interfaces provide a one-click method to close a tab, typically either a button at an end of the tab bar or on the tab itself. The SDT currently lacks both. The only way to close a tab is to right-click on the tab and choose "Close" from the pop-up menu, or choose "Close All" from the "File" menu, which closes all of the open tabs except for the "Scenario" tab. A one-click method of closing a tab should be provided.

3. CyberCIEGE Game

Having been played by several people up to this point, the CyberCIEGE game itself has already had many problems worked out. At present, there is just one area that ought to be reviewed more thoroughly. Late in the development process for this scenario, a change was made that allows the user to deselect all of the password length options, indicating that the user has the option of not having a password. It is not obvious to the player that this is a possibility, as none of the other sets of buttons, such as password change frequency or character complexity, give the player the option of having none selected. Indeed, never requiring the password to be changed is an explicit option. In order to improve consistency as well as better display all of the player's options, a specific "no password" option should be displayed.

B. CONCLUSION

This thesis set out to develop a scenario that would provide the player with some insights into issues surrounding the development of password policies. Such a scenario was developed. Comments from the testers who played the scenario indicate that it was mostly successful in providing this, though additional refinement, as outlined in the previous section, would be helpful.

The secondary goal of this thesis was to perform testing of the Scenario Development Tool. This testing contributed to improvements in the functionality and usability of the tool, through the submission of bug reports as well as suggestions for improvements. Further refinement should further increase the value of the tool.

As computer security issues enter the public consciousness, the need for tools to educate people about them will continue to grow. It is hoped that this research will help to fill one small piece of that need.

APPENDIX A. SCENARIO SOURCE CODE LISTING

The following is the code listing for the scenario as played by the student testers. It is presented in the form of the Scenario Definition File generated by the SDT and used by the CyberCIEGE game.

```
//FILE:TomsHiLo.CSM
//DESIGNER:nobody
SDFid: TomsHiLo.CSM 8/2/05 9 55 AM :end
Organization:
      Name: Tom's Tools :end
      Title: Hi/Low Password Settings :end
      StartMonth: 4 :end
      StartDay: 10 :end
      StartHour: 8 :end
      StartMinute: 0 :end
      StartMoney: 10000 :end
      Budget: 5000 :end
      ProfitSharing: 10 :end
      MainOfficeVersion: large :end
      OffsiteOfficeVersion: small_office :end
      WorkSpaceFile: workspacemft1.txt :end
      Internet: true :end
      InternetStatic: false :end
      EndOnCompromise: false :end
      EasyTraining: false :end
      TutorialAttacks: false :end
      QuitText: Giving up? :end
:end //of Organization

Site:
      Name: Simple Office :end
      Description: Tom's Tools building :end
:end  //of Site

Options:
      UseScenarioCatalogItems: YES :end
      NonServerDefaultPublicAccess: YES :end
      NetworksEverywhere: YES :end
      GuardCostsAtStartup: NO :end
:end
Camera:
      ViewCenterX: 55 :end
      ViewCenterY: 41 :end
      ViewAmountZoom: 2 :end
      ViewAmountAngle: 0 :end
:end // of Camera

AttackMasks:
      Mask: 0 :end
      Mask: 0 :end
      Mask: 0 :end
      Mask: 0 :end
      Mask: 1 :end
      Mask: 1 :end
      Mask: 0 :end
      Mask: 0 :end
      Mask: 1 :end
      Mask: 1 :end
      Mask: 1 :end
      Mask: 1 :end
      Mask: 1 :end
      Mask: 1 :end
```

```
      Mask: 0 :end
      Mask: 1 :end
      Mask: 0 :end
      Mask: 0 :end
      Mask: 0 :end
      Mask: 0 :end
      Mask: 0 :end
:end // of attackMask
Network:
      Name: Lan1 :end
      NetID: 2.4.7...0 :end
:end //of Network

Network:
      Name: Lan2 :end
      NetID: 0.0.0..0 :end
:end //of Network

Network:
      Name: Lan3 :end
      NetID: 0.0.0..0 :end
:end //of Network

Network:
      Name: HO :end
      NetID: 3.0.0..0 :end
:end //of Network

Network:
      Name: HO1 :end
      NetID: 4.0.0..0 :end
:end //of Network

Network:
      Name: HO2 :end
      NetID: 4.0.0..0 :end
:end //of Network

Department:
      Name: Employees :end
:end //of Department

Zone:
      Name: Entire Office :end
      Description:  :end
      Site: Simple Office :end
      Art: ..\testing\art\defaultoffice.tga :end
      Static: false :end
      // Start Default Component Settings
            HoldsUserAsset: true :end
            ProtectWithACL: false :end
            WriteDownPasswords: true :end
            LockorLogoff: false :end
            PasswordLength: short :end
            PasswordCharacterSet: any :end
            PasswordChangeFrequency: never :end
            NoEmailAttachmentExecute: true :end
```

```
            NoExternalSoftware: true :end
            NoUseOfModems: false :end
            NoWebMail: false :end
            NoMediaLeaveZone: false :end
            ApplyPatches: false :end
            LeaveMachinesOn: false :end
            NoPhysicalModifications: false :end
            UserBackup: false :end
      // End Default Component Settings
      Receptionist: false :end
      GuardAtDoor: false :end
      PatrollingGuard: false :end
      ProhibitMedia: false :end
      ProhibitPhoneDevices: false :end
      ExpensivePerimeterAlarms: false :end
      ModeratePerimeterAlarms: false :end
      Re-enforcedWalls: false :end
      SurveillanceCameras: false :end
      PermitEscortedVisitors: false :end
      VisualPeopleInspection: false :end
      XrayPackages: false :end
      KeyLockOnDoor: false :end
      CipherLockOnDoor: false :end
      ExpensiveIrisScanner: false :end
      ModerateIrisScanner: false :end
      Badges: false :end
      Order: 0 :end
      PermittedUsers: *.Public :end
      ULC:  19 51 :end
      LRC:  68 25 :end
      DoorGuardFacing: NORTH :end
:end //of Zone

Zone:
      Name: Walled Office South East :end
      Description:  :end
      Site: Simple Office :end
      Art: ..\testing\art\LowRightZone.tga :end
      Static: false :end
      // Start Default Component Settings
            HoldsUserAsset: true :end
            ProtectWithACL: false :end
            WriteDownPasswords: true :end
            LockorLogoff: false :end
            PasswordLength: short :end
            PasswordCharacterSet: any :end
            PasswordChangeFrequency: never :end
            NoEmailAttachmentExecute: true :end
            NoExternalSoftware: true :end
            NoUseOfModems: false :end
            NoWebMail: false :end
            NoMediaLeaveZone: false :end
            ApplyPatches: false :end
            LeaveMachinesOn: false :end
            NoPhysicalModifications: false :end
            UserBackup: false :end
      // End Default Component Settings
```

```
      Receptionist: false :end
      GuardAtDoor: false :end
      PatrollingGuard: false :end
      ProhibitMedia: false :end
      ProhibitPhoneDevices: false :end
      ExpensivePerimeterAlarms: true :end
      ModeratePerimeterAlarms: false :end
      Re-enforcedWalls: true :end
      SurveillanceCameras: false :end
      PermitEscortedVisitors: false :end
      VisualPeopleInspection: false :end
      XrayPackages: false :end
      KeyLockOnDoor: false :end
      CipherLockOnDoor: false :end
      ExpensiveIrisScanner: false :end
      ModerateIrisScanner: false :end
      Badges: false :end
      Order: 0 :end
      PermittedUsers: *.Management :end
      ULC:  49 38 :end
      LRC:  68 26 :end
      DoorGuardFacing: NORTH :end
:end //of Zone

Zone:
      Name: Offsite :end
      Description:  :end
      Site: Simple Office :end
      Art: ..\testing\art\nothing.tga :end
      Static: true :end
      // Start Default Component Settings
            HoldsUserAsset: true :end
            ProtectWithACL: true :end
            WriteDownPasswords: false :end
            LockorLogoff: true :end
            PasswordLength: medium :end
            PasswordCharacterSet: any :end
            PasswordChangeFrequency: never :end
            NoEmailAttachmentExecute: false :end
            NoExternalSoftware: false :end
            NoUseOfModems: false :end
            NoWebMail: true :end
            NoMediaLeaveZone: false :end
            ApplyPatches: true :end
            LeaveMachinesOn: false :end
            NoPhysicalModifications: true :end
            UserBackup: false :end
      // End Default Component Settings
      Receptionist: true :end
      GuardAtDoor: false :end
      PatrollingGuard: false :end
      ProhibitMedia: false :end
      ProhibitPhoneDevices: false :end
      ExpensivePerimeterAlarms: true :end
      ModeratePerimeterAlarms: false :end
      Re-enforcedWalls: true :end
      SurveillanceCameras: true :end
```

```
      PermitEscortedVisitors: false :end
      VisualPeopleInspection: false :end
      XrayPackages: false :end
      KeyLockOnDoor: true :end
      CipherLockOnDoor: true :end
      ExpensiveIrisScanner: false :end
      ModerateIrisScanner: true :end
      Badges: true :end
      Order: 0 :end
      ULC:  94 29 :end
      LRC:  106 21 :end
      DoorGuardFacing: NORTH :end
:end //of Zone

Secrecy:
      Name: Non-sensitive Data :end
      Description:  Non-sensitive  information  with  no  protection
requirements beyond the discretionary access controls. :end
      Level: 1 :end
      SecrecyValue: 0 :end
      AttackerValue: 0 :end
      InitialBackGroundCheck: None :end
:end //of Secrecy

Secrecy:
      Name: Business Confidential :end
      Description:  :end
      Level: 4 :end
      Category: 5 :end
      SecrecyValue: 10000 :end
      AttackerValue: 0 :end
      InitialBackGroundCheck: High :end
:end //of Secrecy

DACGroups:
      Group: Management :end
      InitialBackGroundCheck: High :end
      Group: Staff :end
      InitialBackGroundCheck: High :end
      Group: Public :end
      InitialBackGroundCheck: None :end
:end // of DAC Groups
Asset:
      Name: Web Page :end
      Description: Tom's Tools Web Page :end
      IsInstantiated: true :end
      HasDAC: true :end
      DOSMotive: 0 :end
      AvailabilityPenalty: 0 :end
      AccessList:
            *.Public YNNN           *.Public YNNN
      :end
      CostList:
            Access: *.Public :end
            AccessMode: NYNN :end
            Cost: 0 :end
            AttackerMotive: 0 :end
```

```
      :end
      CostList:
            Access: *.Public :end
            AccessMode: NYNN :end
            Cost: 0 :end
            AttackerMotive: 0 :end
      :end
:end //of Asset

Asset:
      Name: Basic Research :end
      Description: Public info on the web :end
      IsInstantiated: false :end
      HasDAC: true :end
      Secrecy: Non-sensitive Data :end
      DOSMotive: 0 :end
      AvailabilityPenalty: 0 :end
      AccessList:
            *.Management YYYY       *.Staff YYYY
      :end
      CostList:
            Access: *.Management :end
            AccessMode: NNNN :end
            Cost: 0 :end
            AttackerMotive: 0 :end
      :end
:end //of Asset

Asset:
      Name: Inventory :end
      Description: Current store inventory :end
      IsInstantiated: true :end
      HasDAC: true :end
      Secrecy: Business Confidential :end
      DOSMotive: 0 :end
      AvailabilityPenalty: 0 :end
      AccessList:
            *.Management YYNN
      :end
      CostList:
            Access: *.Management :end
            AccessMode: NNNN :end
            Cost: 0 :end
            AttackerMotive: 0 :end
      :end
:end //of Asset

Asset:
      Name: Customer Emails :end
      Description: Email inqueries from customers. :end
      IsInstantiated: true :end
      HasDAC: true :end
      Secrecy: Business Confidential :end
      DOSMotive: 0 :end
      AvailabilityPenalty: 0 :end
      AccessList:
            *.Management YYNN       *.Staff YYNN
```

```
      :end
      CostList:
            Access: *.Management :end
            AccessMode: NNNN :end
            Cost: 0 :end
            AttackerMotive: 0 :end
      :end
:end //of Asset

AssetGoal:
      Name: Read Inventory :end
      Description: Read access to the Inventory. :end
      Shared: false :end
      Asset:
            Name: Inventory :end
            filtered: false :end
            AccessMode: YXXX :end
      :end
      AvailabilityCostPenalty: 0 :end
:end //of AssetGoal

AssetGoal:
      Name: Write Inventory :end
      Description: Write access to the Inventory. :end
      Shared: false :end
      Asset:
            Name: Web Page :end
            filtered: false :end
            AccessMode: XYXX :end
      :end
      AvailabilityCostPenalty: 0 :end
:end //of AssetGoal

AssetGoal:
      Name: Access E-Mail :end
      Description: Read and write customer emails. :end
      Shared: true :end
      Asset:
            Name: Customer Emails :end
            filtered: false :end
            AccessMode: YYXX :end
      :end
      SoftwareType: EMAIL CLIENT :end
      AvailabilityCostPenalty: 0 :end
:end //of AssetGoal

User:
      Name: Tom :end
      Dept:  Employees :end
      SecrecyClearance:  Business Confidential :end
      DACGroups:
            Management :end
            Staff :end
      :end
      DefaultDAC: Management :end
      AssetGoal:
            AssetGoalName: Write Inventory :end
```

```
            TargetUsage: 50 :end
            Happiness: 15 :end
            Productivity: 25 :end
      :end
      AssetGoal:
            AssetGoalName: Read Inventory :end
            TargetUsage: 50 :end
            Happiness: 25 :end
            Productivity: 25 :end
      :end
      AssetGoal:
            AssetGoalName: Access E-Mail :end
            TargetUsage: 50 :end
            Happiness: 10 :end
            Productivity: 10 :end
      :end
      Trustworthiness:  100 :end
      InitialTraining: 70 :end
      Happiness: 50 :end
      Productivity: 50 :end
      HISupportSkill: 10 :end
      PosIndex: 4 :end
      Cost: 1 :end
      Gender: male :end
      UserDescription: Tom is the owner of Tom's Tools. :end
:end //of User

User:
      Name: Jane :end
      Dept:  Employees :end
      SecrecyClearance:  Business Confidential :end
      DACGroups:
            Staff :end
      :end
      DefaultDAC: Staff :end
      AssetGoal:
            AssetGoalName: Read Inventory :end
            TargetUsage: 50 :end
            Happiness: 25 :end
            Productivity: 25 :end
      :end
      AssetGoal:
            AssetGoalName: Access E-Mail :end
            TargetUsage: 50 :end
            Happiness: 25 :end
            Productivity: 50 :end
      :end
      Trustworthiness:  75 :end
      InitialTraining: 70 :end
      Happiness: 50 :end
      Productivity: 50 :end
      HISupportSkill: 10 :end
      PosIndex: 0 :end
      Cost: 1 :end
      Gender: female :end
      UserDescription: Jane handles most of the customer service and
sales tasks for Tom's Tools. :end
```

```
:end //of User

User: //SupportStaff
      Name: Steve :end
      Dept:  Tech :end
      HWSupportSkill: 90 :end
      SWSupportSkill: 90 :end
      HISupportSkill: 90 :end
      Trustworthiness:  90 :end
      InitialTraining: 95 :end
      Happiness: 90 :end
      Productivity: 90 :end
      Skill: 95 :end
      PosIndex: 1 :end
      Cost: 1000 :end
      Gender: Male :end
      UserDescription: Steve writes operating systems in his free time.
:end
:end //of SupportStaff

User: //SupportStaff
      Name: Boris :end
      Dept:  Security :end
      HWSupportSkill: 10 :end
      SWSupportSkill: 10 :end
      HISupportSkill: 90 :end
      Trustworthiness:  90 :end
      InitialTraining: 95 :end
      Happiness: 90 :end
      Productivity: 90 :end
      Skill: 95 :end
      PosIndex: 2 :end
      Cost: 1000 :end
      Gender: Male :end
      UserDescription: Boris bench presses small jets. :end
:end //of SupportStaff

Workspace:
      PosIndex: 0 :end
:end

Workspace:
      PosIndex: 1 :end
:end

Workspace:
      PosIndex: 2 :end
:end

Workspace:
      PosIndex: 3 :end
:end

Workspace:
      PosIndex: 4 :end
:end
```

```
Workspace:
      PosIndex: 5 :end
      Type: Server :end
:end

Workspace:
      PosIndex: 14 :end
:end

Component: //start of the physical component section.
      Name: Web Server :end
      IsTemplate: false :end
      Description: Web server :end
      AssetProtection: false :end
      HW: Targo Server :end
      Cost: 2000 :end
      Resale: 600 :end
      Maintenance: 20 :end
      Availability: 99 :end
      Static: true :end
      OS: Populos V9 Server :end
      Software: Populos Web Slave :end
      RemoteAuthentication: true :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: true :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: true :end
      BlockRemovableMedia: false :end
      EnforcePasswordPolicy: false :end
      BlockLocalStorage: false :end
      BrowserSettings: Loose :end
      EmailSettings: Loose :end
      UpdatePatches: AsReleased :end
      ManagedAntivirus: false :end
      User:  :end
      PosIndex: 14 :end
      Assets: Web Page :end
      Assets: Customer Emails :end
      AccessListLocal: *.Public :end
      AccessListRemote: *.Public :end
      UninterruptiblePower: false :end
      CM: Weak :end
      //NetworkConnections:
      Network:
            Name: HO1 :end
      :end //of network description
      //end of NetworkConnections:
      ComponentProceduralSettings:
            HoldsUserAsset: true :end
```

```
            ProtectWithACL: false :end
            WriteDownPasswords: false :end
            LockorLogoff: true :end
            PasswordLength: long :end
            PasswordCharacterSet: complex :end
            PasswordChangeFrequency: two :end
            NoEmailAttachmentExecute: true :end
            NoExternalSoftware: true :end
            NoUseOfModems: true :end
            NoWebMail: true :end
            NoMediaLeaveZone: true :end
            ApplyPatches: true :end
            LeaveMachinesOn: true :end
            NoPhysicalModifications: true :end
            UserBackup: false :end
      :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
      Name: BitFlipper Router HO :end
      IsTemplate: false :end
      Description: Simple Router :end
      AssetProtection: false :end
      HW: Bit Flipper :end
      Cost: 2000 :end
      Resale: 600 :end
      Maintenance: 20 :end
      Availability: 99 :end
      Static: true :end
      OS: FlipOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      EnforcePasswordPolicy: false :end
      BlockLocalStorage: false :end
      BrowserSettings: Loose :end
      EmailSettings: Loose :end
      UpdatePatches: AsReleased :end
      ManagedAntivirus: false :end
      User:  :end
      PosIndex: 14 :end
      UninterruptiblePower: false :end
      CM: Weak :end
      //NetworkConnections:
      Network:
            Name: HO1 :end
```

```
      :end //of network description
      //end of NetworkConnections:
      Network:
            Name: Internet :end
      :end //of network description
      //end of NetworkConnections:
:end //of physical component Section

Component: //start of the physical component section.
      Name: Intranet Server :end
      IsTemplate: false :end
      Description: Intranet server :end
      AssetProtection: false :end
      HW: Targo Server :end
      Cost: 2000 :end
      Resale: 600 :end
      Maintenance: 20 :end
      Availability: 99 :end
      Static: false :end
      OS: Populos V9 Server :end
      Software: Populos Web Slave :end
      Software: Extortos :end
      RemoteAuthentication: true :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: true :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: true :end
      BlockRemovableMedia: false :end
      EnforcePasswordPolicy: false :end
      BlockLocalStorage: false :end
      BrowserSettings: Loose :end
      EmailSettings: Loose :end
      UpdatePatches: AsReleased :end
      ManagedAntivirus: false :end
      User:  :end
      PosIndex: 5 :end
      Assets: Inventory :end
      AccessListLocal: *.Management :end
      AccessListRemote: *.Management :end
      AccessListRemote: *.Staff :end
      UninterruptiblePower: false :end
      CM: Weak :end
      //NetworkConnections:
      Network:
            Name: Lan1 :end
      :end //of network description
      //end of NetworkConnections:
      ComponentProceduralSettings:
            HoldsUserAsset: true :end
```

```
            ProtectWithACL: false :end
            WriteDownPasswords: false :end
            LockorLogoff: true :end
            PasswordLength: long :end
            PasswordCharacterSet: complex :end
            PasswordChangeFrequency: two :end
            NoEmailAttachmentExecute: true :end
            NoExternalSoftware: true :end
            NoUseOfModems: true :end
            NoWebMail: true :end
            NoMediaLeaveZone: true :end
            ApplyPatches: true :end
            LeaveMachinesOn: true :end
            NoPhysicalModifications: true :end
            UserBackup: false :end
      :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
      Name: BitFlipper Router Office :end
      IsTemplate: false :end
      Description: Office router :end
      AssetProtection: false :end
      HW: Bit Flipper :end
      Cost: 2000 :end
      Resale: 600 :end
      Maintenance: 20 :end
      Availability: 99 :end
      Static: true :end
      OS: FlipOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      EnforcePasswordPolicy: false :end
      BlockLocalStorage: false :end
      BrowserSettings: Loose :end
      EmailSettings: Loose :end
      UpdatePatches: AsReleased :end
      ManagedAntivirus: false :end
      User:  :end
      PosIndex: 5 :end
      UninterruptiblePower: false :end
      CM: Weak :end
      //NetworkConnections:
      Network:
            Name: Lan1 :end
```

```
      :end //of network description
      //end of NetworkConnections:
      Network:
            Name: Internet :end
      :end //of network description
      //end of NetworkConnections:
:end //of physical component Section

Component: //start of the physical component section.
      Name: Toms Targo :end
      IsTemplate: false :end
      Description: Targo Worksaver computer, for use by Tom. :end
      AssetProtection: false :end
      HW: Targo Worksaver :end
      Cost: 2000 :end
      Resale: 600 :end
      Maintenance: 20 :end
      Availability: 99 :end
      Static: false :end
      OS: Populos V9 Desktop :end
      Software: WordSmyth :end
      Software: Internet Contemplator :end
      Software: Extortos :end
      Software: Euphoria :end
      Software: Cell Life :end
      RemoteAuthentication: true :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: true :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: true :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: true :end
      BlockRemovableMedia: false :end
      EnforcePasswordPolicy: true :end
      BlockLocalStorage: false :end
      BrowserSettings: Normal :end
      EmailSettings: Normal :end
      UpdatePatches: AsReleased :end
      ManagedAntivirus: false :end
      User: Tom :end
      PosIndex: 4 :end
      AccessListLocal: Tom :end
      UninterruptiblePower: false :end
      CM: Weak :end
      //NetworkConnections:
      Network:
            Name: Lan1 :end
      :end //of network description
      //end of NetworkConnections:
      ComponentProceduralSettings:
            HoldsUserAsset: true :end
```

```
            ProtectWithACL: false :end
            WriteDownPasswords: true :end
            LockorLogoff: false :end
            PasswordLength: short :end
            PasswordCharacterSet: any :end
            PasswordChangeFrequency: never :end
            NoEmailAttachmentExecute: true :end
            NoExternalSoftware: true :end
            NoUseOfModems: false :end
            NoWebMail: false :end
            NoMediaLeaveZone: false :end
            ApplyPatches: false :end
            LeaveMachinesOn: false :end
            NoPhysicalModifications: false :end
            UserBackup: false :end
      :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
      Name: Janes Targo :end
      IsTemplate: false :end
      Description: Targo Worksaver computer, for use by Jane. :end
      AssetProtection: false :end
      HW: Targo Worksaver :end
      Cost: 2000 :end
      Resale: 600 :end
      Maintenance: 20 :end
      Availability: 99 :end
      Static: false :end
      OS: Populos V9 Desktop :end
      Software: WordSmyth :end
      Software: Internet Contemplator :end
      Software: Extortos :end
      Software: Euphoria :end
      Software: Cell Life :end
      RemoteAuthentication: true :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: true :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: true :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: true :end
      BlockRemovableMedia: false :end
      EnforcePasswordPolicy: true :end
      BlockLocalStorage: false :end
      BrowserSettings: Normal :end
      EmailSettings: Normal :end
      UpdatePatches: AsReleased :end
      ManagedAntivirus: false :end
      User: Jane :end
      PosIndex: 0 :end
```

```
      AccessListLocal: Jane :end
      UninterruptiblePower: false :end
      CM: Weak :end
      //NetworkConnections:
      Network:
            Name: Lan1 :end
      :end //of network description
      //end of NetworkConnections:
      ComponentProceduralSettings:
            HoldsUserAsset: true :end
            ProtectWithACL: false :end
            WriteDownPasswords: true :end
            LockorLogoff: false :end
            PasswordLength: short :end
            PasswordCharacterSet: any :end
            PasswordChangeFrequency: never :end
            NoEmailAttachmentExecute: true :end
            NoExternalSoftware: true :end
            NoUseOfModems: false :end
            NoWebMail: false :end
            NoMediaLeaveZone: false :end
            ApplyPatches: false :end
            LeaveMachinesOn: false :end
            NoPhysicalModifications: false :end
            UserBackup: false :end
      :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the catalog component section.
      Name: Blato Desktop Select :end
      IsTemplate: true :end
      Description: Packed with applications, memory and disk :end
      AssetProtection: false :end
      HW: Blato Desktop Select :end
      Cost: 1700 :end
      Resale: 200 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: NORMAL :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
```

```
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Targo Worksaver :end
      IsTemplate: true :end
      Description: Full suite of productivity software, adequate memory
and dis. :end
      AssetProtection: false :end
      HW: Targo Worksaver :end
      Cost: 1700 :end
      Resale: 200 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Trusted Targo Worksaver :end
      IsTemplate: true :end
      Description: Similar to the Targo Worksaver, but includes the
Trusted Populos OS. :end
      AssetProtection: false :end
      HW: Trusted Targo Worksaver :end
      Cost: 2500 :end
      Resale: 200 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Trusted Populos Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
```

```
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: The Thin Man :end
      IsTemplate: true :end
      Description: A thin client intended to work with either Gossamer
products or Populos Terminal Servers. :end
      AssetProtection: false :end
      HW: The Thin Man :end
      Cost: 900 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos Embedded V5 :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Green Net Client :end
      IsTemplate: true :end
      Description:  A  thin  client  intended  to  work  with  Gossamer
products. Intended use is to connect to multiple networks of different
sensitivity levels :end
      AssetProtection: false :end
      HW: Green Net Client :end
      Cost: 3000 :end
      Resale: 1000 :end
      Maintenance: 100 :end
      Availability: 99 :end
```

```
      OS: Secure Shade Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Lunitos AFOS :end
      IsTemplate: true :end
      Description: Sleek colorful desktop machine with adequate memory
and disk :end
      AssetProtection: false :end
      HW: Lunitos AFOS :end
      Cost: 2300 :end
      Resale: 300 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Lunitos Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Greenshade Client :end
```

```
      IsTemplate: true :end
      Description: High assurance client workstation :end
      AssetProtection: false :end
      HW: Blato Desktop Select :end
      Cost: 4200 :end
      Resale: 800 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Secure Shade Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Targo Server :end
      IsTemplate: true :end
      Description: Full featured server with the worlds most popular
operating system. :end
      AssetProtection: false :end
      HW: Targo Server :end
      Cost: 15000 :end
      Resale: 5000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
```

```
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Blato Server :end
      IsTemplate: true :end
      Description: Full featured server with the worlds most popular
operating system. :end
      AssetProtection: false :end
      HW: Blato Server :end
      Cost: 15000 :end
      Resale: 5000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Twist Off Server :end
      IsTemplate: true :end
      Description: Server class machine with the Jar Lid Server O/S
:end
      AssetProtection: false :end
      HW: Twist Off Server :end
      Cost: 10000 :end
      Resale: 5000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Jar Lid Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
```

```
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Green Shade Server :end
      IsTemplate: true :end
      Description: Server class machine with the Secure Shade Server
high assurance operating system :end
      AssetProtection: false :end
      HW: Green Shade Server :end
      Cost: 80000 :end
      Resale: 20000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Secure Shade Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Mail Appliance :end
      IsTemplate: true :end
      Description: Simple Email Server. :end
      AssetProtection: false :end
      HW: Targo Server :end
      Cost: 5000 :end
      Resale: 2000 :end
      Maintenance: 100 :end
```

```
      Availability: 99 :end
      OS: Jar Lid Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Populos Letter Pusher :end
      IsTemplate: true :end
      Description: Email Server that rules. :end
      AssetProtection: false :end
      HW: Blato Server :end
      Cost: 20000 :end
      Resale: 8000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Web Appliance :end
```

```
      IsTemplate: true :end
      Description: Simple web server :end
      AssetProtection: false :end
      HW: Twist Off Server :end
      Cost: 1500 :end
      Resale: 2000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Jar Lid Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Populos Internet Slave :end
      IsTemplate: true :end
      Description: Web Server that rules the web. :end
      AssetProtection: false :end
      HW: Blato Server :end
      Cost: 10000 :end
      Resale: 2000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
```

```
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: MergerTech DeskProp :end
      IsTemplate: true :end
      Description: Priner :end
      AssetProtection: false :end
      HW: MergerTech DeskProp :end
      Cost: 200 :end
      Resale: 2 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: MergerTech SOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Bit Flipper :end
      IsTemplate: true :end
      Description: High performance router :end
      AssetProtection: false :end
      HW: Bit Flipper :end
      Cost: 150 :end
      Resale: 60 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: FlipOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
```

```
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Bit Flipper VPN :end
      IsTemplate: true :end
      Description: VPN Gateway -- another Bit Flipper product :end
      AssetProtection: false :end
      HW: Bit Flipper VPN :end
      Cost: 200 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: FlipOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Bent Line VPN :end
      IsTemplate: true :end
      Description: VPN Gateway Evaluated to EAL4+ :end
      AssetProtection: false :end
      HW: Bent Line VPN :end
      Cost: 1500 :end
      Resale: 2000 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V8 Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
```

```
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Green Shade VPN :end
      IsTemplate: true :end
      Description: VPN Gateway On a Green Shade Core :end
      AssetProtection: false :end
      HW: Green Shade VPN :end
      Cost: 1500 :end
      Resale: 500 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Green Shade Core :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Crack This! :end
      IsTemplate: true :end
      Description: Best Selling VPN Gateway :end
      AssetProtection: false :end
      HW: Crack This! :end
```

```
      Cost: 1500 :end
      Resale: 500 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Server :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Bit Flipper Switch :end
      IsTemplate: true :end
      Description: Best Selling VPN Gateway :end
      AssetProtection: false :end
      HW: Bit Flipper Switch :end
      Cost: 500 :end
      Resale: 200 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: FlipOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section
```

```
Component: //start of the catalog component section.
      Name: Swenthabit :end
      IsTemplate: true :end
      Description: Vanilla LAN switch :end
      AssetProtection: false :end
      HW: Swenthabit :end
      Cost: 500 :end
      Resale: 200 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: FlipOS :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Five Inches of Asbestos :end
      IsTemplate: true :end
      Description: Best selling firewall :end
      AssetProtection: false :end
      HW: Five Inches of Asbestos :end
      Cost: 900 :end
      Resale: 200 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
```

```
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Bit Flipper Border :end
      IsTemplate: true :end
      Description: Full featured firewall :end
      AssetProtection: false :end
      HW: Bit Flipper Border :end
      Cost: 200 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Wire Stuff :end
      IsTemplate: true :end
      Description: High quality hub with high reliability :end
      AssetProtection: false :end
      HW: Wire Stuff :end
      Cost: 150 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
```

```
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Box with Wires :end
      IsTemplate: true :end
      Description: General purpose hub :end
      AssetProtection: false :end
      HW: Box with Wires :end
      Cost: 90 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Paint It Black :end
      IsTemplate: true :end
      Description:  Link  Encryptor  handles  most  wide  area  network
protocols :end
      AssetProtection: false :end
      HW: Paint It Black :end
      Cost: 290 :end
      Resale: 100 :end
      Maintenance: 100 :end
```

```
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
      Name: Enigma2000 :end
      IsTemplate: true :end
      Description:  Link  Encryptor  handles  most  wide  area  network
protocols :end
      AssetProtection: false :end
      HW: Enigma2000 :end
      Cost: 290 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
```

```
      Name: NightShade :end
      IsTemplate: true :end
      Description:  Link  Encryptor  handles  most  wide  area  network
protocols :end
      AssetProtection: false :end
      HW: NightShade :end
      Cost: 290 :end
      Resale: 100 :end
      Maintenance: 100 :end
      Availability: 99 :end
      OS: Populos V9 Desktop :end
      RemoteAuthentication: false :end
      AcceptPKICerts: false :end
      UseOneTimePasswordToken: false :end
      UseBiometrics: false :end
      UseTokenPKICerts: false :end
      UseClientPKICerts: false :end
      VPNClient: false :end
      ScanEmailAttachments: false :end
      StripEmailAttachments: false :end
      AutomaticLockLogout: false :end
      SelfAdminister: false :end
      SelfAdministerMAC: false :end
      AdministerSoftwareControl: false :end
      BlockRemovableMedia: false :end
      BlockLocalStorage: false :end
      BrowserSettings: LOOSE :end
      EmailSettings: LOOSE :end
      UpdatePatches: NONE :end
      UpdateAntivirus: NONE :end
:end //of catalog component Section

Conditions:
      Condition:
            Tagname: MinCash0 :end
            ConditionClass: MinCashOnHand :end
            Parameter: 0 :end
:end //of Condition

      Condition:
            Tagname: Time36Hours :end
            ConditionClass: TimeCondition :end
            Parameter: 36 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time0days :end
            ConditionClass: TimeCondition :end
            Parameter: 0 :end
:end //of Condition

      Condition:
            Tagname: time30days :end
            ConditionClass: TimeCondition :end
            Parameter: 720 :end
            Parameter: 1 :end
```

```
:end //of Condition

      Condition:
            Tagname: time2days :end
            ConditionClass: TimeCondition :end
            Parameter: 48 :end
:end //of Condition

      Condition:
            Tagname: time1day :end
            ConditionClass: TimeCondition :end
            Parameter: 24 :end
:end //of Condition

      Condition:
            Tagname: time3hours :end
            ConditionClass: TimeCondition :end
            Parameter: 3 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time2hours :end
            ConditionClass: TimeCondition :end
            Parameter: 2 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time4hours :end
            ConditionClass: TimeCondition :end
            Parameter: 4 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time8hours :end
            ConditionClass: TimeCondition :end
            Parameter: 8 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time7hours :end
            ConditionClass: TimeCondition :end
            Parameter: 7 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time12hours :end
            ConditionClass: TimeCondition :end
            Parameter: 12 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
```

```
            Tagname: time1hour :end
            ConditionClass: TimeCondition :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time1hourPhase :end
            ConditionClass: TimeCondition :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time5hours :end
            ConditionClass: TimeCondition :end
            Parameter: 5 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time6hours :end
            ConditionClass: TimeCondition :end
            Parameter: 6 :end
            Parameter: 1 :end
:end //of Condition

      Condition:
            Tagname: time3days :end
            ConditionClass: TimeCondition :end
            Parameter: 72 :end
:end //of Condition

      Condition:
            Tagname: TomShortPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  PasswordLength:Short :end
:end //of Condition

      Condition:
            Tagname: TomAnyCharPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  PasswordCharacterSet:Any :end
:end //of Condition

      Condition:
            Tagname: TomNeverChgPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  PasswordChangeFrequency:never :end
:end //of Condition

      Condition:
            Tagname: JaneNeverChgPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
```

```
            SecondConditionText:  PasswordChangeFrequency:never :end
:end //of Condition

      Condition:
            Tagname: JaneAnyCharPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
            SecondConditionText:  PasswordCharacterSet:Any :end
:end //of Condition

      Condition:
            Tagname: JaneShortPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
            SecondConditionText:  PasswordLength:Short :end
:end //of Condition

      Condition:
            Tagname: JaneLongPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
            SecondConditionText:  PasswordLength:Long :end
:end //of Condition

      Condition:
            Tagname: JaneComplexCharPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
            SecondConditionText:  PasswordCharacterSet:Complex :end
:end //of Condition

      Condition:
            Tagname: Jane2MChgPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
            SecondConditionText:  PasswordChangeFrequency:two :end
:end //of Condition

      Condition:
            Tagname: JaneWritePass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Jane :end
            SecondConditionText:  WriteDownPassword: :end
:end //of Condition

      Condition:
            Tagname: TomWritePass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  WriteDownPassword: :end
:end //of Condition

      Condition:
            Tagname: Tom2MChgPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  PasswordChangeFrequency:two :end
```

```
:end //of Condition

      Condition:
            Tagname: TomCompexCharPass :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  PasswordCharacterSet:Complex :end
:end //of Condition

      Condition:
            Tagname: Phase1Done :end
            ConditionClass: PhaseCompleted :end
            ConditionText: First :end
:end //of Condition

      Condition:
            Tagname: Phase2Done :end
            ConditionClass: PhaseCompleted :end
            ConditionText: Second :end
:end //of Condition

      Condition:
            Tagname: MedPWSet :end
            ConditionClass: ObjectiveCompleted :end
            ConditionText: MedPWSettings :end
:end //of Condition

      Condition:
            Tagname: HighPWSet :end
            ConditionClass: ObjectiveCompleted :end
            ConditionText: HighPWSettings :end
:end //of Condition

      Condition:
            Tagname: HighPWAccept :end
            ConditionClass: ObjectiveCompleted :end
            ConditionText: HighPWUsersAccept :end
:end //of Condition

      Condition:
            Tagname: TomTrain75 :end
            ConditionClass: UserTraining :end
            ConditionText: Tom :end
            Parameter: 75 :end
            Parameter: 100 :end
:end //of Condition

      Condition:
            Tagname: JaneTrain75 :end
            ConditionClass: UserTraining :end
            ConditionText: Jane :end
            Parameter: 75 :end
            Parameter: 100 :end
:end //of Condition

      Condition:
            Tagname: TomLongPass :end
```

```
            ConditionClass: AssignedComputerHas :end
            ConditionText: Tom :end
            SecondConditionText:  PasswordLength:Long :end
:end //of Condition

:end
Triggers:
      Trigger:
            TriggerName: JaneLowPassHack :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
            ConditionList:    time1hour    AND    JaneShortPass    AND
JaneNeverChgPass AND JaneAnyCharPass AND_NOT Phase1Done :end
            TriggerText:  Jane's  password  settings  are  too  low;  an
Internet hacker was able to break into her computer and read the
Inventory. Cost $1000. :end
            Parameter: -1000 :end
      :end //of Trigger

      Trigger:
            TriggerName: goPhase2 :end
            TriggerClass: SetPhase :end
            FrequencyInDays: 999 :end
            FixedDelay: 0 :end
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList: MedPWSet :end
            TriggerText: Second :end
            SecondTriggerText: You've started to notice a pattern to
the break-in attempts. The attacks are coming from an address range
that can be traced to Hammer House, the more established hardware store
in town. You suspect that they've hired hackers to try and break in and
modify your Inventory. You see from your server logs that their attack
method  seems  to  be  to  brute  force  attack  the  passwords  on  Tom  and
Jane's computers. Keep them out long enough to gather enough evidence
to use against them in court. :end
      :end //of Trigger

      Trigger:
            TriggerName: goPhase2Cash :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: 999 :end
            FixedDelay: 0 :end
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList: MedPWSet :end
            Parameter: 30000 :end
      :end //of Trigger

      Trigger:
            TriggerName: MedPWObjCompleted :end
            TriggerClass: SetObjectiveStatus :end
            FrequencyInDays: 999 :end
            FixedDelay: 0 :end
```

```
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList: NOT ((JaneShortPass AND JaneNeverChgPass AND
JaneAnyCharPass)   OR   (JaneLongPass   AND   JaneComplexCharPass   AND
Jane2MChgPass)    OR    (TomShortPass    AND    (TomNeverChgPass    OR
TomAnyCharPass))   OR   (TomLongPass   AND   TomCompexCharPass   AND
Tom2MChgPass)) :end
            TriggerText: MedPWSettings :end
            Parameter: 1 :end
      :end //of Trigger

      Trigger:
            TriggerName: HihgPWObjCompleted :end
            TriggerClass: SetObjectiveStatus :end
            FrequencyInDays: 999 :end
            FixedDelay: 0 :end
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList:    Phase1Done    AND    JaneLongPass    AND
JaneComplexCharPass   AND   Jane2MChgPass   AND   Tom2MChgPass   AND
TomCompexCharPass AND TomLongPass AND TomWritePass AND JaneWritePass
:end
            TriggerText: HighPWSettings :end
            Parameter: 1 :end
      :end //of Trigger

      Trigger:
            TriggerName: UsersAcceptHighPWObjCompleted :end
            TriggerClass: SetObjectiveStatus :end
            FrequencyInDays: 999 :end
            FixedDelay: 0 :end
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList: TomTrain75 AND JaneTrain75 :end
            TriggerText: HighPWUsersAccept :end
            Parameter: 1 :end
      :end //of Trigger

      Trigger:
            TriggerName: LoseBroke :end
            TriggerClass: LoseTrigger :end
            FrequencyInDays: 999 :end
            FixedDelay: 0 :end
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList: MinCash0 :end
            TriggerText: Tom's Tools ran out of money and was forced to
close. You're out of a job. :end
      :end //of Trigger

      Trigger:
            TriggerName: TomLowPassHack :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
```

```
            ConditionList:     time1hour     AND     TomShortPass     AND
(TomNeverChgPass OR TomAnyCharPass) AND_NOT Phase1Done :end
            TriggerText:  Tom's  password  settings  are  too  low;  an
Internet  hacker  was  able  to  break  into  his  computer  and  read  the
Inventory. Cost $10000. :end
            Parameter: -10000 :end
      :end //of Trigger

      Trigger:
            TriggerName: TomHiighPassForget :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
            ConditionList:     time1hour     AND     TomLongPass     AND
TomCompexCharPass   AND   Tom2MChgPass   AND_NOT   TomWritePass   AND_NOT
TomTrain75 :end
            TriggerText:  Tom's  password  settings  are  too  high,  he
forgot it and you had to reset it for him. Cost: $50. :end
            Parameter: -50 :end
      :end //of Trigger

      Trigger:
            TriggerName: JaneHighPassForget :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
            ConditionList:     time1hour     AND     JaneLongPass     AND
JaneComplexCharPass  AND  Jane2MChgPass  AND_NOT  JaneWritePass  AND_NOT
JaneTrain75 :end
            TriggerText:  Jane's  password  settings  are  too  high,  she
forgot it and you had to reset it for her. Cost: $50. :end
            Parameter: -50 :end
      :end //of Trigger

      Trigger:
            TriggerName: JaneHighPassWritten :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
            ConditionList:     time1hour     AND     JaneLongPass     AND
JaneComplexCharPass   AND   Jane2MChgPass   AND   JaneWritePass   AND_NOT
JaneTrain75 AND_NOT Phase1Done :end
            TriggerText: Jane's password settings are too high, she had
it written down and a customer saw it. Cost: $1000 :end
            Parameter: -1000 :end
      :end //of Trigger

      Trigger:
            TriggerName: ReadAttack :end
            TriggerClass: CashTrigger :end
            FrequencyInDays: .25 :end
```

```
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
            ConditionList:    Phase1Done    AND    time1hour    AND_NOT
((JaneLongPass    AND    JaneComplexCharPass    AND    Jane2MChgPass)    OR
JaneWritePass) :end
            TriggerText: Jane's computer was broken into and someone
from Hammer House was able to read the Inventory. Cost $30,000. :end
            Parameter: -30000 :end
      :end //of Trigger

      Trigger:
            TriggerName: InvWriteAttack :end
            TriggerClass: LoseTrigger :end
            FrequencyInDays: .5 :end
            FixedDelay: 0 :end
            RandomDelay: .25 :end
            RunsWhilePaused: false :end
            ConditionList:    Phase1Done    AND    time1hour    AND_NOT
(TomLongPass AND TomCompexCharPass AND Tom2MChgPass) :end
            TriggerText: Tom's computer was broken into and someone
from Hammer House was able to change the store Inventory. Because of
this attack, Tom's Tools is forced to close and you're out of a job.
:end
      :end //of Trigger

      Trigger:
            TriggerName: Win :end
            TriggerClass: WinTrigger :end
            FrequencyInDays: 999 :end
            FixedDelay: .25 :end
            RandomDelay: 0 :end
            RunsWhilePaused: false :end
            ConditionList: HighPWAccept AND HighPWSet :end
            TriggerText: With password settings at their highest, you
were able to thwart Hammer House's attack attempts long enough to
gather enough evidence to get a court injunction against Hammer House
and their hackers. Things are returning to normal at Tom's Tools, and
business is increasing as the media attention drives business away from
Hammer House. :end
      :end //of Trigger

      Trigger:
            TriggerName: SellNails :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .05 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Jane sells a box of nails. :end
      :end //of Trigger

      Trigger:
            TriggerName: SellPlywood :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .25 :end
```

```
            FixedDelay: 0 :end
            RandomDelay: .1 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Tom sells several sheets of plywood. :end
      :end //of Trigger

      Trigger:
            TriggerName: SellScrewdriver :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .06 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Jane sells a screwdriver and a case of screws.
:end
      :end //of Trigger

      Trigger:
            TriggerName: SellSaw :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .09 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Jane sells a power saw. :end
      :end //of Trigger

      Trigger:
            TriggerName: JobApp :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .5 :end
            FixedDelay: 0 :end
            RandomDelay: .1 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Tom receives a job application in his e-mail.
:end
      :end //of Trigger

      Trigger:
            TriggerName: SellLightBulbs :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .25 :end
            FixedDelay: 0 :end
            RandomDelay: .11 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Jane sells a bundle of light bulbs. :end
      :end //of Trigger

      Trigger:
            TriggerName: SellCordlessDrill :end
            TriggerClass: TickerTrigger :end
            FrequencyInDays: .25 :end
```

```
            FixedDelay: 0 :end
            RandomDelay: .08 :end
            RunsWhilePaused: false :end
            ConditionList: NOT Phase2Done :end
            TriggerText: Tom sells a cordless drill. :end
      :end //of Trigger

:end
Phases:
Phase:
      TagName: First :end
      DisplayName: Configure password settings. :end
      CompletedText: Password settings look good, neither too loose nor
too strict. :end
      UncompletedText: ... :end
      PhaseCompleted: false :end
 :end //of Phase

Phase:
      TagName: Second :end
      DisplayName: Lock down component password settings. :end
      CompletedText: Password settings are now at their highest and the
users accept this. :end
      UncompletedText: ... :end
      PhaseCompleted: false :end
 :end //of Phase

:end
Objectives:
Objective:
      TagName: MedPWSettings :end
      DisplayName: Configure password settings. :end
      Phase: 0 :end
      CompletedText: Password settings look good. :end
      UncompletedText: Password settings still need work. :end
:end //of Objective

Objective:
      TagName: HighPWSettings :end
      DisplayName: Lock down component password settings. :end
      Phase: 1 :end
      CompletedText: Password settings look good. :end
      UncompletedText: Password settings still need work. :end
:end //of Objective

Objective:
      TagName: HighPWUsersAccept :end
      DisplayName: Users accept the password settings. :end
      Phase: 1 :end
      CompletedText: Users accept the password settings. :end
      UncompletedText: Users dislike the password settings. :end
:end //of Objective

:end
ShortBriefing:
      Tom's Tools is a new tool selling business. Computer break-in
attempts have caused them to hire you to replace their previous
```

computer consultant, who didn't have a security background. You need to configure the password settings on Tom and Jane's computers so that they can work without password policy issues coming up. (PARAGRAPH) See the Objectives and Game tab for more information.
:end

Briefing:
You need to manage the password settings on Tom and Jane's computers. They need to be able to work for a while without password policy issues coming up in order to advance to the next phase. (PARAGRAPH) Since this is a small business, the users need remote access so they can access the system when they are not in the store. Workstations also need Internet access so they can access e-mail to answer customer and vendor inquiries; the e-mail server is located off site at a co-location facility.
:end

:EndOfFile

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PLAYER EVALUATIONS

The following pages reproduce the evaluations completed by students who played the scenario. Player responses are italicized.

CyberCIEGE – Tom's Tools scenario player evaluation

Thank you for taking the time to evaluate the Tom's Tools scenario for CyberCIEGE.

In order to play the game, you will need to mount the Windows share containing CyberCIEGE:

Open **My Computer**, and in the box next to **Address**, enter **\\kiska\Groups2$\CyberCIEGE**

Open "**Password Policies.bat"** and follow the directions.

Please be aware that when you play the game, some of the results from playing will be saved to a log file for later evaluation.

What do you think the game was attempting to teach?

The game was attempting to teach good password composition techniques and that passwords are susceptible to attacks, such as brute force.

If you were already aware of these issues, do you think that someone who is not might learn something from it?

I think this scenario is definitely good for teaching someone about password security.

As a game, did you enjoy playing it? If not, what would improve your enjoyment of it?

I enjoyed playing it…maybe making the text in the objectives tab more descriptive would be helpful. Overall though good job ☺

CyberCIEGE – Tom's Tools scenario player evaluation

Thank you for taking the time to evaluate the Tom's Tools scenario for CyberCIEGE.

In order to play the game, you will need to mount the Windows share containing CyberCIEGE:

Open **My Computer**, and in the box next to **Address**, enter **\\kiska\Groups2$\CyberCIEGE**

Open "**Password Policies.bat"** and follow the directions.

Please be aware that when you play the game, some of the results from playing will be saved to a log file for later evaluation.

What do you think the game was attempting to teach?

Phase1: Configure Password
It would be nice to describe what sort of password policy that the company is adopting.

It would be nice to have a short description or guide the user to understand the Short, Medium, Long password length mean. This would apply to Password Character Set, Change Password Every. This will be useful for beginner.

There is no indication that the user has successfully completed the objective 1.
There is some error on the Zone Tab. If click on it, the whole game is terminated.
Encounter a couple of crashes (Not too such what happen, maybe it is the server)

If I only set the password configuration on "Janes" computer only, the game allow me to proceed to the next Phase. Is that right? I presume that the policy should apply throughout the Company.

Phase 2: Lock down component password settings.
I am not sure what does this objective meant. I did not finish the game as I am stuck here.

If you were already aware of these issues, do you think that someone who is not might learn something from it?

This can be used to re-enforce the ideas because a professional IT may sometime overlook the fundamental stuff.

As a game, did you enjoy playing it? If not, what would improve your enjoyment of it?

I think it would be nice to have more guidance.

CyberCIEGE – Tom’s Tools scenario player evaluation

Thank you for taking the time to evaluate the Tom’s Tools scenario for CyberCIEGE.

In order to play the game, you will need to mount the Windows share containing CyberCIEGE:

Open **My Computer**, and in the box next to **Address**, enter **\\kiska\Groups2$\CyberCIEGE**

Open “**Password Policies.bat”** and follow the directions.

Please be aware that when you play the game, some of the results from playing will be saved to a log file for later evaluation.

What do you think the game was attempting to teach?

Phase 1: The need for password control.
a) Set the password length (must be medium, too high, play forget)
b) Set the password complexity (medium)
c) Set the frequency of change (2 months)

Phase 2: Lock Down Component Password Setting.
I am having some problem regarding the objective of phase you. Can you provide more details?

If you were already aware of these issues, do you think that someone who is not might learn something from it?

As a game, did you enjoy playing it? If not, what would improve your enjoyment of it?

Ø Note that the Zone tab crashes the application.
Ø Actually, the objectives are met for phase 1 if I configure only Jane's computer. However it does not work it I configure Tom's only. Think need to check both Tom's and Jane's computers to achieve objectives.

CyberCIEGE – Tom's Tools scenario player evaluation

Thank you for taking the time to evaluate the Tom's Tools scenario for CyberCIEGE.

In order to play the game, you will need to mount the Windows share containing CyberCIEGE:

Open **My Computer**, and in the box next to **Address**, enter **\\kiska\Groups2$\CyberCIEGE**

Open "**Password Policies.bat"** and follow the directions.

Please be aware that when you play the game, some of the results from playing will be saved to a log file for later evaluation.

What do you think the game was attempting to teach?

That if you make your password policy too complex, that you will undermine the goals of the security program. If you make it too weak, then you are vulnerable to attack.

If you were already aware of these issues, do you think that someone who is not might learn something from it?

Maybe, maybe not…I think there needs to be more instruction in the game…Are you going to include any feedback mechanisms in the scenario?

As a game, did you enjoy playing it? If not, what would improve your enjoyment of it?

No, I felt lost. I had no idea that it was phase two and there were new objectives.

More directions on the first objective on what is expected.
What is the 2nd objective trying to communicate?

Why can't I enforce password policy on the web server?

I need more feedback…of course, too much limits the gameplaying enjoyment…hmmm what a dilemma.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[Adams 1999] Adams, A. and Sasse, M. A. (1999, December). "Users Are Not The Enemy." *Communications of the ACM*, vol. 42, no. 12, pp. 40-46.

[Altova 2005] *XMLSpy 2005*. Altova, release 3. Retrieved July 2005 from the World Wide Web: http://www.altova.com/products_ide.html

[Bickel 2003] Bickel, R., Cook, M., Haney, J., Kerr, M. Parker, T., and Pares, H. (2003, December). *Guide to Securing Microsoft Windows XP*. National Security Agency, Operational Network Evaluations Division of the Systems and Network Attack Center. Retrieved September 2005 from the World Wide Web: http://www.nsa.gov/snac/os/winxp/winxp.pdf

[Bishop 1991] Bishop, M. (1991, February). "Password Management." *Compcon Spring 1991 Digest of Papers*, San Francisco, California, pp. 167-169.

[Bishop 1995] Bishop, M. and Klein, D. V. (1995). "Improving System Security via Proactive Password Checking." *Computers & Security*, vol. 14, no. 3, pp. 233-249.

[Bown 2004] Bown, M. (2004, September). *Password Management*. Safecoms. Retrieved August 2005 from the World Wide Web: http://www.safecoms.com.au/resources/newsletters/september2004/password/

[CISR 2005] Naval Postgraduate School Center for Information Systems Security Studies and Research. (2005). *CyberCIEGE Scenario Development Tool User's Guide*.

[ComponentSoftware 2005] *CSDiff*. ComponentSoftware, version 5.0. Retrieved September 2005 from the World Wide Web: http://www.componentsoftware.com/Products/CSDiff/

[Davis 1989] Davis, F. D. (1989, September). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly*, vol. 13, no. 3, pp. 319-340.

[Dierks 1999] Dierks, T. and Allen, C. (1999, January). *RFC 2246: The TLS Protocol, Version 1.0*. Internet Engineering Task Force, Network Working Group. Retrieved September 2005 from the World Wide Web: http://www.ietf.org/rfc/rfc2246.txt

[Feldmeier 1990] Feldmeier, D. C. and Karn, P. R. (1990, January). "UNIX Password Security – Ten Years Later." *Lecture Notes in Computer Science*, vol. 435, pp. 44-63.

[Ferguson 1998] Ferguson, P. and Huston, G. (1998, April). "What is a VPN?" *OPENSIG'98 Workshop on Open Signaling for ATM, Internet, and Mobile Networks*, Toronto, Canada.

[Ferré 2001] Ferré, X., Juristo, N., Windul, H., and Constantine, L. (2001, January/February). "Usability Basics for Software Developers." *IEEE Software*, vol. 18, no. 1, pp. 22-29.

[Ganesan 1994] Ganesan, R. and Davies, C. (1994, October). "A New Attack on Random Pronounceable Password Generators." *17th National Computer Security Conference*, Baltimore, Maryland.

[Garris 2002] Garris, R., Ahlers, R., and Driskell, J. E. (2002, December). "Games, Motivation, and Learning: A Research and Practice Model." *Simulation & Gaming*, vol. 33, no. 4, pp. 441-467.

[Irvine 2004] Irvine, C. E. and Thompson, M. F. (2004, July). "Expressing an Information Security Policy Within a Security Simulation Game." *Proceedings of the Sixth Workshop on Education in Computer Security*, Monterey, California, pp. 43-49.

[Irvine 2005] Irvine, C. E., Thompson, M. F., and Allen, K. (2005, May/June). "CyberCIEGE: Gaming for Information Assurance." *IEEE Security & Privacy Magazine*, vol. 3, no. 3, pp. 61-64.

[Johns 2004] Johns, K. W. (2004). *Toward Managing & Automating CyberCIEGE Scenario Definition File Creation*. Master of Science Thesis, Department of Computer Science, Naval Postgraduate School, Monterey, California.

[Kurzban 1985] Kurzban, S. A. (1985). "Easily Remembered Passphrases—A Better Approach." *ACM SIGSAC Review*, vol. 3, no. 2-4, pp. 10-21.

[LaMore 2004] LaMore, R. L. (2004). *CyberCEIGE Scenario Illustrating Secrecy Issues Through Mandatory and Discretionary Access Control Policies in a Multi-Level Security Network*. Master of Science Thesis, Department of Computer Science, Naval Postgraduate School, Monterey, California.

[Levine 2004] Levine, J. G., Grizzard, J. B., and Owen, H. L. (2004, November/December). "Using Honeynets to Protect Large Enterprise Networks." *IEEE Security & Privacy Magazine*, vol. 2, no. 6, pp. 73-75.

[Loshin 2001] Loshin, P. (2001, June). "Sealing the Pipes." *Information Security*. Retrieved September 2005 from the World Wide Web: http://infosecuritymag.techtarget.com/articles/june01/features_protocols.shtml

[Microsoft 2004] Hypertext (2004). *The Microsoft Windows User Experience*. Microsoft Corporation. Retrieved August 2005 from the World Wide Web: http://msdn.microsoft.com/library/en-us/dnwue/html/welcome.asp

[Neff 2003] Neff, G. and Stark, D. (2003). "Permanently Beta: Responsive Organization in the Internet Era" in *Society Online: The Internet in Context*, Howard, P. N. and Jones, S., eds., pp. 173-188. Thousand Oaks, CA: Sage. Retrieved August 2005 from the World Wide Web: http://www.sociology.columbia.edu/people/faculty/stark/papers/permanently_beta.pdf

[NIST 1985] Hypertext (1985). *Federal Information Processing Standards Publication 112 – Password Usage*. United States Department of Commerce, National Institute of Standards and Technology. Retrieved August 2005 from the World Wide Web: http://www.itl.nist.gov/fipspubs/fip112.htm

[NIST 1995] Hypertext (1995, October). *NIST Special Publication 800-12 – An Introduction to Computer Security: The NIST Handbook*. United States Department of Commerce, National Institute of Standards and Technology.

Retrieved August 2005 from the World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html

[O'Gorman 2003] O'Gorman, L. (2003, December). "Comparing Passwords, Tokens, and Biometrics for User Authentication." *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2019-2040.

[Prensky 2001] Prensky, M. (2001). "Simulations: Are They Games?" in *Digital Game-Based Learning*. New York: McGraw-Hill. Retrieved August 2005 from the World Wide Web: http://www.marcprensky.com/writing/Prensky%20-%20Simulations-Are%20They%20Games.pdf

[Rivermind 2004] Rivermind, Inc. (2004). *Scenario Format Template*, version 15m.

[Saltzer 1975] Saltzer, J. H. and Schroeder, M. D. (1975, September). "The Protection of Information in Computer Systems." *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308.

[Shinder 2003] Shinder, D. (2003). *Passwords: The Weak Link in Network Security*. WindowSecurity.com. Retrieved August 2005 from the World Wide Web: http://www.windowsecurity.com/articles/Passwords_Network_Security.html

[Sonnenberg 2003] Sonnenberg, A. (2003, June). *SSO: Enabling an Effective Password Policy*. Imprivata, Inc. Retrieved August 2005 from the World Wide Web: http://www.infosec.co.uk/files/White_Paper_2003_imprivata_password_policy.pdf

[Thompson 2005] Thompson, M. F. (2005, August). "RE: Chapter 2, 8/24." Personal e-mail.

[Warren 2003] Warren, D. (2003). *Course Notes for CS3600: Introduction to Information Assurance (IA): Computer Security*. Naval Postgraduate School, Monterey, California.

[Yan 2001] Yan, J. J. (2001, September). "A Note on Proactive Password Checking." *Proceedings of the 2001 Workshop on New Security Paradigms*, Cloudcroft, New Mexico, pp. 127-135.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Ken Allen
   Rivermind, Inc
   Mountain View, CA

4. Hugo A. Badillo
   NSA
   Fort Meade, MD

5. George Bieber
   OSD
   Washington, DC

6. RADM Joseph Burns
   Fort George Meade, MD

7. John Campbell
   National Security Agency
   Fort Meade, MD

8. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

9. CDR Daniel L. Currie
   PMW 161
   San Diego, CA

10. Louise Davidson
    National Geospatial Agency
    Bethesda, MD

11. Vincent J. DiMaria
    National Security Agency
    Fort Meade, MD

12. LCDR James Downey
NAVSEA
Washington, DC

13. Scott Gallardo
Rivermind, Inc
Mountain View, CA

14. Dr. Diana Gant
National Science Foundation

15. Jennifer Guild
SPAWAR
Charleston, SC

16. Richard Hale
DISA
Falls Church, VA

17. LCDR Scott D. Heller
SPAWAR
San Diego, CA

18. Wiley Jones
OSD
Washington, DC

19. Russell Jones
N641
Arlington, VA

20. David Ladd
Microsoft Corporation
Redmond, WA

21. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

22. Steve LaFountain
NSA
Fort Meade, MD

23. Dr. Greg Larson
IDA
Alexandria, VA

24. Penny Lehtola
NSA
Fort Meade, MD

25. Gilman Louie
In-Q-Tel
Menlo Park, CA

26. Ernest Lucier
Federal Aviation Administration
Washington, DC

27. CAPT Deborah McGhee
Headquarters U.S. Navy
Arlington, VA

28. Dr. Vic Maconachy
NSA
Fort Meade, MD

29. Doug Maughan
Department of Homeland Security
Washington, DC

30. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

31. John Mildner
SPAWAR
Charleston, SC

32. Jim Roberts
Central Intelligence Agency
Reston, VA

33. Charles Sherupski
Sherassoc
Round Hill, VA

34. Dr. Ralph Wachter
ONR
Arlington, VA

35. David Wennergren
DoN CIO
Arlington, VA

36. David Wirth
N641
Arlington, VA

37. Daniel Wolf
NSA
Fort Meade, MD

38. Jim Yerovi
NRO
Chantilly, VA

39. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

40. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

41. Paul C. Clark
Naval Postgraduate School
Monterey, CA

42. Michael Thompson
Naval Postgraduate School
Monterey, CA

43. David S. Mueller
Civilian, Naval Postgraduate School
Monterey, CA